Bochumer Masterarbeiten

2014

MASTER KRIMINOLOGIE UND POLIZEIWISSENSCHAFT

Anne Katharina Wonsack

Skimming

Die Täter im kriminologischen Blickfeld

E-Book
www.felix-verlag.de

ISBN 978-3-86293-100-2

RUHR-UNIVERSITÄT BOCHUM
JURISTISCHE FAKULTÄT

Masterstudiengang Kriminologie und Polizeiwissenschaft

MASTERARBEIT
zur Erlangung des akademischen Grades
„Master of Arts in Criminology and Police Science“

Skimming:
Die Täter im kriminologischen Blickfeld

Vorgelegt von:	Anne Katharina Wonsack
Matrikelnummer:	108 111 202 429
Erstgutachterin:	Professorin Dr. Britta Bannenberg
Zweitgutachter:	Professor PhDr. Uli Rothfuss
Abgabedatum:	20.02.2014

Inhaltsverzeichnis

Abkürzungsverzeichnis

AG	Amtsgericht
ATM	Automated/automatic teller machine
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BGH	Bundesgerichtshof
BKA	Bundeskriminalamt
BZR	Bundeszentralregister
CCC	Chaos Computer Club
COMECON	Council for Mutual Economic Assistance
DNA	Desoxyribonukleinsäure
ENISA	Europäische Agentur für Netz- und Informationssicherheit
EMV	Europay International, MasterCard und Visa
EKS	EURO Kartensysteme GmbH
FreizügG/EU	Freizügigkeitsgesetz/EU
GAA	Geldausgabeautomaten
IMF	International Monetary Fund
IWF	Internationaler Währungsfonds
MM-Merkmal	Moduliertes, maschinenlesbares Merkmal
OCG	Organised crime gang/group
PIN	Persönliche Identifikationsnummer
PKS	Polizeiliche Kriminalstatistik
POS	Point of sale
RGW	Rat für gegenseitige Wirtschaftshilfe
SEPA	Single Euro Payment Area
SIS	Schengener Informationssystem
StA	Staatsanwaltschaft
StGB	Strafgesetzbuch
StR	Strafsenat
StPO	Strafprozessordnung
ULSIT	University of Library Studies and Information Technologies
ZDS	Zentralen Debit-Schadensbekämpfung

1. Einleitung

„*Angriff der Karten-Kloner*“ (Bachfeld 2007) oder „*Skimming-Welle: Betrug am Bankautomaten boomt wie nie*“ (Hendrich 2010) – Schlagzeilen wie diese finden sich regelmäßig in Zeitungen oder im Internet. Vor allem die Schadenssummen lassen in vielen dieser Fälle aufhorchen. Allein etwa 1,4 Millionen Euro konnten Täter in einem Fall in Hessen abgreifen. Hier wurden die Zahlungsgeräte eines Baumarktes manipuliert und somit die Bankdaten von insgesamt 721 Kunden ausgespäht (Helfrich 2009). Diese Tatbegehungsweise wird als „Skimming“[1] bezeichnet. Hierunter ist die Manipulation von Geldautomaten bzw. POS-Terminalgeräten[2] zur Erlangung von Bankdaten sowie der sich anschließenden Gelderlangung mittels Kartendubletten zu verstehen. Dabei gibt es mannigfaltige Ausführungen, manipuliert werden neben Geldautomaten und Terminalgeräten auch Fahrkartenautomaten oder vollautomatische Zapfsäulen mit integrierter Zahlfunktion.

Zuletzt wurde bekannt, dass Täter sogar direkt die Hardware von Geldautomaten angriffen. Hierzu schnitten sie ein Loch in die Verkleidung des Geldautomaten, um einen USB-Stick an den Computer im Inneren anbringen zu können. Über den USB-Stick infizierten sie den Rechner mit Malware. Nun konnten sie den Geldautomaten über die Tastatur steuern und sich beliebige Geldbeträge auszahlen lassen. Das Loch in der Verkleidung des Automaten verschlossen sie wieder. Die Bank bemerkte die Tat erst, als sie sich über fehlende Bargeldbestände wunderte und zusätzliche Überwachungskameras anbringen ließ. Die Täter konnten „auf frischer Tat“ festgenommen und ein USB-Stick mit der entsprechenden Software sichergestellt werden: Kürzlich präsentierten Sicherheitsforscher, denen die Entschlüsselung des Software-Codes gelang, das Vorgehen der Täter und die Software auf einem Kongress, der vom Chaos Computer Club (CCC) ausgerichtet wurde (heiseSecurity 2014).

[1] Englisch to skim – etwas abschöpfen

[2] Englisch Point of Sale – Verkaufspunkt. Etwa im Einzelhandel werden Terminalgeräte eingesetzt, um dem Kunden ein bargeldloses Bezahlen zu ermöglichen. Aus Perspektive des Verkäufers handelt es sich bei dem point of sale um den Verkaufspunkt. Im Alltag bedeutet dies zumeist die Kasse eines Geschäfts. Im Folgenden vereinfacht als Terminalgerät bezeichnet.

1.1 Problemdarstellung

Die dargestellten Sachverhalte lassen die stete Aktualität des Deliktphänomens Skimming erkennen. Hinzu kommt, dass Zahlungen immer häufig bargeldlos abgewickelt werden und folglich ein höheres Schadensrisiko besteht. Dies ist beispielsweise an der Zunahme der Anzahl an Geldautomaten in Deutschland zu erkennen, lediglich im Jahr 2012 war ein leichter Rückgang zu verzeichnen.

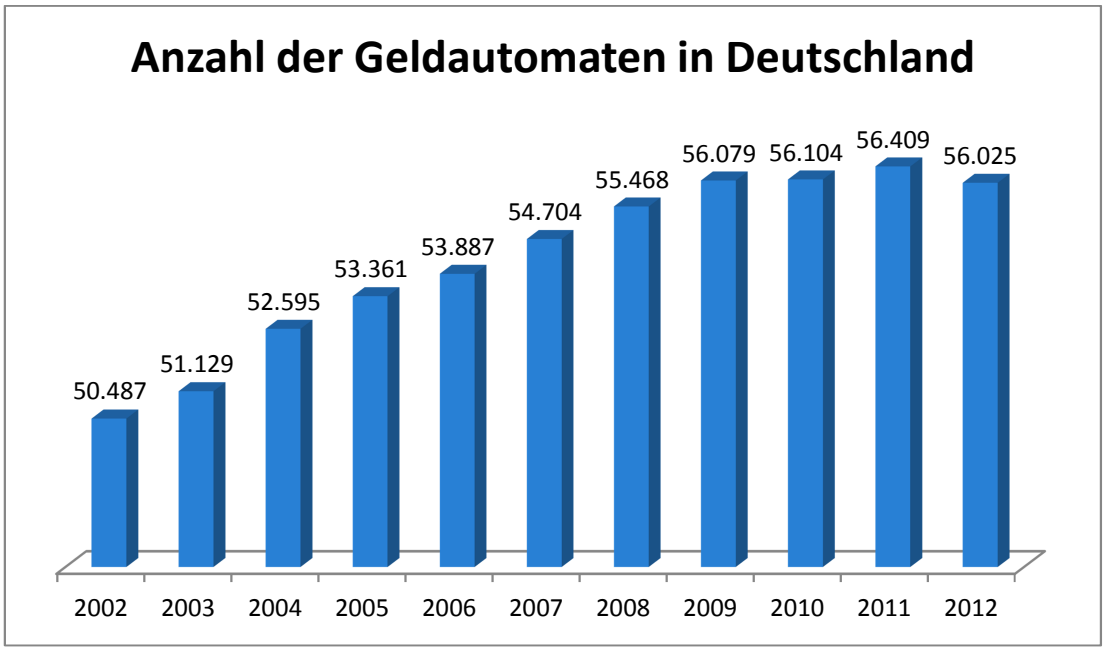


Abbildung 1: Anzahl der Geldautomaten in Deutschland
(Bundesverband deutscher Banken 2013)

Bislang finden sich in der Literatur Abhandlungen zur strafrechtlichen Problematik sowie zur kriminalistischen Vorgehensweise, meist ausgerichtet auf die polizeiliche Sachbearbeitung. Die Phänomenologie, gerade im Hinblick auf die Täter, wurde dabei bislang kaum untersucht (Bachmann und Goeck 2011, S. 153). Insbesondere hinsichtlich der Tatsache, dass die Täter bzw. Tatverdächtigen nahezu ausschließlich aus den südosteuropäischen Ländern Bulgarien und Rumänien stammen. Deutsche Staatsangehörige oder Staatsangehörige anderer Nationen bilden im Deliktsfeld Skimming die Ausnahme (Bundeskriminalamt 2013a, S. 9). Somit wird ein lukratives Delikt nahezu ausschließlich von Staatsangehörigen zweier Länder verübt. Dies scheint äußerst bemerkenswert und soll daher den Schwerpunkt dieser kriminologisch ausgerichteten Abhandlung bilden.

1.2 Forschungsleitende Frage

Um ein geeignetes methodisches Vorgehen wählen zu können, ist die Formulierung einer forschungsleitenden Frage erforderlich. Diese im Mittelpunkt der Untersuchung stehende Frage lautet:

Warum werden Skimming-Straftaten nahezu ausschließlich von bulgarischen oder rumänischen Staatsangehörigen verübt?

Diese offen verfasste Fragestellung bedingt eine explorativ angelegte Methodik, da der zu erforschende Bereich weitgehend unbekannt ist und hinsichtlich der kriminologisch ausgerichteten Fragestellung keine Vermutung vorliegt (vgl. Diekmann 2007, S. 33). Der Untersuchungsgegenstand soll erst entdeckt werden, eine Hypothesengenerierung wird angestrebt. Insofern werden im weiteren Verlauf bei einer induktiven Herangehensweise vorwiegend qualitative Erhebungsinstrumente eingesetzt.

1.3 Aufbau der Arbeit

Zu Beginn erfolgt die Darstellung des Deliktes Skimming hinsichtlich Tatbegehungsweise, strafrechtlicher Einordnung, statistischer Daten sowie des aktuellen deutschsprachigen und internationalen Forschungsstandes. Nach diesen grundlegenden Informationen schließt sich der empirische Teil mit den Erhebungsinstrumenten qualitativ-quantitative Inhaltsanalyse sowie qualitative Befragung/qualitatives Interview an. Hierbei wird das methodische Vorgehen im Einzelnen erläutert, die Ergebnisse werden dargestellt und analysiert. Auf die Empirie folgt die Diskussion der Forschungsergebnisse sowie die Generierung von Hypothesen. Zuletzt werden die zentralen Ergebnisse aus Sicht der Verfasserin beschrieben[3].

2. Phänomenologie Skimming

Zur Hinführung auf den empirischen Teil der Arbeit wird das Phänomen Skimming definiert und beschrieben. Nach grundlegender Vorstellung der

[3] Im Verlauf der Arbeit werden immer wieder englischsprachige Texte zitiert. Zum besseren Verständnis findet sich in der Fußnote eines jeden englischen Zitats eine Übersetzung in die deutsche Sprache. Diese wurde von der Verfasserin angefertigt. Sie entsprechen keiner professionellen Übersetzung, geben jedoch den Sinn der Aussage voll umfänglich wieder.

Tatbegehungsweise erfolgt eine kurze strafrechtliche Einordnung. Hiernach folgt eine Aufstellung statistischer Daten. Eine Zusammenfassung des aktuellen Forschungsstands, basierend auf ausgewerteter Literatur, schließt die Darstellung dieses Phänomens ab.

2.1 Definition und Beschreibung

Der Begriff „Skimming“ beschreibt das Abgreifen von Zahlungskarten-Daten sowie den dazugehörigen Persönlichen Identifikationsnummern (=PIN) an Geldausgabeautomaten[4] (GAA) bzw. POS-Terminalgeräten. Die erlangten Bankdaten ermöglichen den Tätern, mit Hilfe von Kartendubletten, Zugang zum Geldbestand fremder Bankkonten zu erlangen. Eine einheitliche Definition für den Begriff Skimming gibt es nicht. Das Phänomen ist seit der Jahrtausendwende bekannt (Kochheim 2012, S. 8) und seitdem demonstrieren die Täter ihre Anpassungsfähigkeit. Die zur Manipulation eingesetzte Hard- und Software fordert Geldinstitute und Verfolgungsbehörden stets neu heraus.

Die Täter benötigen zwei Formen von Daten: Die auf dem Magnetstreifen einer Debit[5]- oder Kreditkarte gespeicherten Angaben zum Bankkonto sowie die Persönliche Identifikationsnummer. Dabei kann das Vorgehen der Täter grob in drei Bereiche eingeteilt werden. Im ersten Schritt wird Zusatzelektronik am Geldautomaten angebracht. Hierbei handelt es sich um ein Magnetstreifenlesegerät, das mit einer Speichereinheit verbunden ist (vgl. Schmidt 2012, S. 15). Diese elektronischen Bauteile werden auf einer Leiterplatte[6] fixiert. Um nicht aufzufallen, wird diese Leiterplatte in Form und Farbe an den jeweiligen Karteneinzugsschacht angepasst. Während ein Bankkunde den manipulierten Geldautomaten zum Abheben von Bargeld nutzt und seine Zahlungskarte in den Karteneinzugsschacht einführt, liest die Zusatzelektronik den Magnetstreifen der Zahlungskarte[7] aus. Der Magnetstreifen besteht aus mehreren sogenannten „Spuren“ und ist gemäß eines ISO-Standards

[4] Im Folgenden vereinfacht als Geldautomat bezeichnet.

[5] Debitkarte: (Lateinisch debere – schulden). Hierbei handelt es sich um eine Bankkarte zur bargeldlosen Bezahlung oder zur Nutzung am Geldausgabeautomaten. Der fällige Betrag wird dem Konto sofort belastet, es wird kein Kredit eingeräumt. Die bekannteste Debitkarte ist die ec-Karte.

[6] Printed circuit board (PCB)

[7] Sofern eine Unterscheidung zwischen Debit- und Kreditkarte für die kriminologische Betrachtung nicht relevant ist, wird fortan der übergeordnete Begriff „Zahlungskarte“ verwendet.

unter anderem mit der Kontonummer und der Bankleitzahl des Bankkunden beschrieben (vgl. Schmidt 2012, S. 15). Neben diesen Daten benötigen die Täter auch die PIN. Sie bringen daher im Bereich des Geldautomaten getarnte Kameras an, um die PIN-Eingabe des Bankkunden zu filmen. Diese beiden Schritte, den Vorgang des „Ausspähens" von Daten, bemerkt der Bankkunde in der Regel nicht, da die Zusatzelektronik kaum zu erkennen ist. Nach einer gewissen Zeit nehmen die Täter ihre Skimming-Technik wieder ab und lesen die gespeicherten Daten aus. In einem weiteren Schritt werden die Daten des Magnetstreifens mit einem im Handel erhältlichen Magnetstreifen-Schreibgerät auf Kartenrohlinge („white plastics") übertragen. Im letzten Schritt werden diese Kartendubletten (counterfeits) zum sogenannten „Cashing"[8] eingesetzt: An ausländischen Geldautomaten werden Geldabhebungen getätigt, bis das finanzielle Limit des genutzten Bankkontos erreicht ist. Dubletten von Kreditkarten werden beispielsweise auch zum Bezahlen an Tankstellen verwendet.

Deutsche Debitkarten verfügen – weltweit einzigartig – über eine besondere technische Sicherheitsvorkehrung, das sogenannte „MM-Merkmal" - moduliertes, maschinenlesbares Merkmal (vgl. Kochheim 2012, S. 15). Hierbei handelt es sich um eine geheime, maschinenlesbare Substanz, die in den Kartenkörper einer originalen Zahlungskarte eingebettet wird. Ein deutscher Geldautomat erkennt, dass es sich um eine deutsche Zahlungskarte handelt und versucht, mit dem MM-Merkmal zu kommunizieren. Gelingt dies nicht, weil das MM-Merkmal fehlt, bricht der Geldautomat den Vorgang ab. Dieses Merkmal gilt bis heute als fälschungssicher (EURO Kartensysteme GmbH). Sogenannte „white plastics" enthalten dieses nicht. Insofern können Fälschungen (Kartendubletten) deutscher Debitkarten nicht an deutschen Geldautomaten, sondern ausschließlich an ausländischen Geldautomaten eingesetzt werden. Seit 2011 müssen Täter ihre Kartenfälschungen zudem im außereuropäischen Ausland einsetzen. Denn seitdem werden Transaktionen im europäischen SEPA-Raum[9] ausschließlich über den Chip autorisiert, nicht mehr über den Magnetstreifen. Da die Täter aber mit Magnetstreifenkarten

[8] Englisch cash – Bargeld/Barmittel
[9] Single Euro Payment Area – Einheitlicher Euro-Zahlungsverkehrsraum

arbeiten, müssen sie das Cashing in sogenannten „Nicht-Chip-Länder“ durchführen (Bundeskriminalamt 2013a, S. 8).

Wenn sich der betroffene Bankkunde bei der Durchsicht seiner Kontoauszüge über Buchungen aus dem Ausland wundert, ist die Tathandlung in der Regel bereits abgeschlossen und die Täter sind im Besitz des Geldes. Für den Bankkunden entsteht letztlich kein Schaden. Meldet er den Vorfall dem kontoführenden Geldinstitut, erhält er Geld in Höhe der unberechtigten Buchungen zurück. Diese Gelder werden aus einem Haftungsfonds der Kreditwirtschaft gezahlt (vgl. Treude 2011, S. 7), welchen die Firma EURO Kartensysteme GmbH[10] (EKS) verwaltet: „*In der bei der EURO Kartensysteme GmbH angesiedelten Zentralen Debit-Schadensbekämpfung (ZDS) erfolgt die zentrale Schadenserfassung, die detaillierte Schadensauswertung und die Abwicklung der Schäden mit Debitkarten*“ .

Um das Cashing erfolgreich betreiben zu können, darf die Manipulation des Geldautomaten nicht auffallen. Insofern muss die Zusatzelektronik optimal an den jeweils manipulierten Geldautomaten angepasst sein. Meist handelt es sich um zwei voneinander getrennte Technikeinheiten. Ein Vorsatzgerät, der sogenannte „Skimmer“ wird am Karteneinzugsschacht angebracht. Anfänglich waren viele Eingangstüren zu Bankfoyers durch ein Türzugangssystem gesichert, welches das Einführen einer Zahlungskarte verlangte. Diese Türöffner konnten alternativ zum Auslesen der Magnetstreifendaten verwendet werden. Aktuell erfolgen die Abgriffe der Daten zumeist am Geldautomaten, da eine Vielzahl von Türöffnern abgebaut bzw. sicherheitstechnisch aufgerüstet wurde (Bundeskriminalamt 2013a, S. 6).
Um die Eingabe der PIN zu filmen bzw. zu speichern, werden zumeist Kameras eingesetzt. Diese werden häufig in Leisten oberhalb des Geldautomaten-Displays angebracht. Alternativ hierzu werden Kameras auch in Rauchmeldern, Prospekthaltern, Deckenleuchten oder anderen, unauffälligen Gegenständen verbaut (vgl. Küch 2010, S. 13). Anstelle einer Kamera kann auch ein Tastaturaufsatz eingesetzt werden. Dieser sehr dünne Aufsatz wird auf

[10] Ein Unternehmen der deutschen Kreditwirtschaft. Homepage: www.eurokartensysteme.de, zuletzt geprüft am 20.02.2014.

den regulären Zahlenblock aufgesetzt. Die in dem Aufsatz verbauten elektronischen Kontakte speichern die Tasten, die der Bankkunde drückt und geben den Tastendruck mechanisch an die Originaltastatur weiter (vgl. Niggl 2010, S. 118).
In aller Regel müssen die Täter zwei Mal am Geldautomaten arbeiten. Anfangs zum Anbauen der Skimming-Technik und nach geraumer Zeit wiederum zum Abbau der Skimming-Technik mit gefüllten Datenspeichern. Es besteht auch die Möglichkeit, dass die abgegriffenen Daten (Kartendaten und PIN-Eingabe) direkt per Funk an die Täter übertragen werden. Die Täter halten sich dazu in der Nähe des Geldautomaten auf, um die Daten mit einem Laptop empfangen und ggf. direkt weiterleiten zu können (vgl. Mujkanovic 2009, S. 43-44). Das Anbringen der Zusatzelektronik erfolgt meist durch sogenannte „Läufer", die zur Tatausführung angeleitet werden. Im Gegensatz zu Montage und Demontage der Elektronik gestaltet sich die Herstellung dieser Geräte „*diffiziler und verlangt elektrotechnisches Know-how*" (Treude 2011, S. 7).

Nach der Montage der Geräte setzen die Täter häufig sogenannte „Testkarten" oder „Prüfkarten" ein. Hierbei handelt es sich um beliebige Plastikkarten mit Magnetstreifen (neben Bankkarten beispielsweise Tankkarten, Karten zum Sammeln von Bonuspunkten). Indem die Täter eine solche Karte in den Karteneinzugsschacht eines Geldautomaten einführen, überprüfen sie den Sitz ihrer Zusatzelektronik. Bei richtiger Justierung wird die Karte reibungslos eingezogen und wieder ausgegeben. Der Einsatz solcher Testkarten kann seitens des Geldinstitutes festgestellt werden, denn grundsätzlich wird jeder Vorgang an einem Geldautomaten registriert und in sogenannten „Journalen" festgehalten. Aus diesen Journalen gehen das Datum, die Uhrzeit, die Bankleitzahl, die Kontonummer sowie diverse weitere Daten hervor. Die oben genannten Testkarten weichen in diesen Daten von üblichen (deutschen) Zahlungskarten ab. Dies ermöglicht es, auffällige Karten zu erkennen. Bei der Firma EKS werden Datensätze auffälliger Karten, die vermutlich Tätern zuzuordnen sind, gesammelt und gespeichert (vgl. Küch 2010, S. 10). Einzelne Geldinstitute gleichen die Listen auffälliger Karten mit ihren Journalen ab. Dies nennt man Testkartenmonitoring oder Testkartenscreening. Hinweise

auf mögliche Manipulation können hierdurch, je nach Anwendung des Geldinstitutes, in Echtzeit oder im Nachgang erkannt werden. Mit der Liste der identifizierten Testkarten arbeiten auch die Ermittlungsbehörden. Ein Abgleich an mehreren Orten und zu unterschiedlichen Zeiten eingesetzter Testkarten ermöglicht das Erkennen von Tatzusammenhängen (vgl. Kuschling und Schober 2013, S. 18-19).

Den Geldinstituten stehen weitere Gegenmaßnahmen zur Verfügung. Neben der Aufklärung und Sensibilisierung von Mitarbeitern und Kunden sowie verstärkter Kontrolle können mechanische und technische Schutzmaßnahmen getroffen werden. So kann das Anbringen eines Sichtschutzes oberhalb des Zahlenblocks das Filmen der PIN-Eingabe erschweren. Zudem ist der Einbau einer zusätzlichen Elektronik, sogenanntes „Anti-Skimming-Modul", im Inneren des Geldautomaten möglich. Diese Elektronik erkennt Skimming-Technik, die auf der Außenseite angebracht wird, „*aufgrund des entstehenden deutlich höheren kapazitiven Magnetfelds*" (Hannich 2007, S. 26). Das Anti-Skimming-Modul baut daraufhin ein „*permanentes Störmagnetfeld*" (ebenda) auf, welches das Lesegerät der Täter stört.

Als weitere Maßnahme gegen Skimming-Straftaten und andere Missbrauchsfälle gilt die Einführung der Chiptechnologie, als Alternative zum Magnetstreifen. Durch die Implementierung eines Chips sollen gespeicherte Daten besser gegen Kopieren und Verfälschung geschützt werden. Seit verpflichtender Nutzung der Chip-Technologie für den SEPA-Zahlungsraum im Jahr 2011 und der damit einhergehenden Einführung des EMV[11]-Standards, wurde eine Art Verursacherprinzip (Haftungsumkehr/liability shift) eingeführt (vgl. EMVCo 2011, S. 8). Ausgangspunkt hierfür ist die Annahme, dass der EMV-Chip fälschungssicher ist. Wurde eine Zahlungskarte mit gefälschtem oder verfälschtem Magnetstreifen eingesetzt, da eine der Transaktionsparteien den Magnetstreifen anstelle des fälschungssicheren EMV-Chips akzeptierte, so trägt diese Transaktionspartei die Haftung für entstandene Schäden. Diese Rege-

[11] **E**uropay International, **M**asterCard und **V**ISA. Standard für Zahlungskarten mit Prozessorchip sowie dazugehörige Chipkarten-Lesegeräte (Geldautomaten, POS-Terminals).

lung gilt für Geldautomaten und POS-Terminals (EURO Kartensysteme GmbH).

Doch solange Zahlungskarten mit Chip und Magnetstreifen ausgegeben werden, können die Täter jedoch die Magnetstreifendaten abgreifen. Das Bundeskriminalamt wirbt daher für die „Magstripe-Controlling"-Strategie. Hierbei ist der Magnetstreifen grundsätzlich deaktiviert, sodass ein Abgreifen der Daten nicht möglich ist. Auf Wunsch kann der Bankkunde den Magnetstreifen vorübergehend aktivieren lassen. Beispielsweise wenn er in ein „Nicht-Chip-Land" reist und dort auf den Magnetstreifen angewiesen ist (Bundeskriminalamt 2013a, S. 10).

Auch im Hinblick auf den Chip ist die Sicherheit fraglich. Wissenschaftler der Universität Cambridge veröffentlichten 2006 einen Versuchsaufbau, wie die Kommunikation einer Chip-Zahlungskarte mit einem Chip-Terminalgerät abgehört und die Daten somit abgegriffen werden können. Dieser Angriff funktioniert nur bei Zahlungskarten, deren Chip mit einem gewissen Verfahren verschlüsselt ist. Andere Verschlüsselungsverfahren gelten derzeit weiterhin als sicher (heiseSecurity 2006). Dennoch zeigt dieser Versuch, dass es sich um ein ständiges „Wettrennen" zwischen Bankinstituten, Strafverfolgungsbehörden und Tätern handelt.

2.2 Strafrechtliche Einordnung

Das Manipulieren eines Geldautomaten und das Einsetzen gefälschter Kartenduplikate verwirklicht mehrere Straftatbestände. Der Bundesgerichtshof hat die Frage hinsichtlich der Strafbarkeit verschiedener Tatausführungshandlungen weitgehend geklärt. Beim Cashing werden die § 263a Abs. 1 StGB (Computerbetrug) und § 152b Abs. 1 StGB[12] (Fälschung von Zahlungskarten mit Garantiefunktion; Verbrechenstatbestand) verwirklicht. Der Schaden entsteht beim Kartenemittenten[13]. Bei deutschen Zahlungskarten

[12] Abgrenzungsmerkmal zu §152a Abs. 1 StGB ist die Garantiefunktion. Hierbei handelt es sich um die Zusage des Kartenemittenten, ungeachtet der aktuellen Zahlungsfähigkeit des Karteninhabers eine Zahlung zu leisten. Zahlungskarten mit Garantiefunktion sind Kredit- und Debitkarten.

[13] Institution, die aufgrund von Bankvorschriften oder internationalen Regularien Zahlungskarten ausgeben darf.

tritt der Schaden im Inland ein, sodass die Tat als Inlandsstraftat zu verfolgen.

Schwieriger gestaltet sich die strafrechtliche Würdigung der Manipulationshandlungen. Der Bundesgerichtshof hat in mehreren Urteilen festgestellt, dass das Abfangen von Kartendaten mittels Skimming-Utensilien kein Ausspähen von Daten im Sinne des § 202a Abs. 1 StGB darstellt. Der 1. Strafsenat begründete dies wie folgt: „*Allerdings ist der Senat der Ansicht, dass die Voraussetzungen des § 202a StGB im vorliegenden Fall jedenfalls dann nicht gegeben sind, wenn die zum Auslesen benutzte Software auch im regulären Handel erhältlich ist*“[14] (BGH, Urteil vom 19.08.2010, 1 Ars 6/10). Der 4. Strafsenat ergänzte: „*Bei den unverschlüsselt auf dem Magnetstreifen gespeicherten Daten fehlt es bereits an einer besonderen Sicherung gegen unberechtigten Zugang, sodass diese Taten als taugliches Tatobjekt im Sinne des § 202 a Abs. 1 StGB ausscheiden.* (…) *Dass Daten magnetisch und damit nicht unmittelbar wahrnehmbar gespeichert sind, stellt keine besondere Sicherung gegen unberechtigten Zugang dar*“ (BGH, Urteil vom 06.07.2010, 4 StR 555/09).

Sobald die Täter die am Geldautomaten abgegriffenen Daten an ihre Mittäter weitergeben, sodass sich eine Fälschung von Zahlungskarten anschließen kann, greift die Versuchsstrafbarkeit im Sinne des § 149 Abs. 1 Nr. 1 StGB. Wobei der BGH noch keine Entscheidung getroffen hat, ob es sich bei den Skimming-Utensilien um „Computerprogramme oder ähnliche Vorrichtungen“ im Sinne des § 149 Abs. 1 StGB handelt.

Möglich ist bei mehreren Tätern auch eine strafbare Einordnung über die Verabredung zu einem Verbrechen im Sinne des § 30 Abs. 2 StGB. In einer Entscheidung des BGH wird nicht auf das Konkurrenzverhältnis eingegangen. Festgestellt wird lediglich: „*Das Anbringen einer Skimming-Apparatur an einem Geldautomaten in der Absicht, dadurch Daten zu erlangen, die später zur Herstellung der Kartendubletten verwendet werden sollen, ist nur eine als solche straflose Vorbereitungshandlung. Die Tat stellt hier daher lediglich eine Verabredung zu dem Verbrechen der banden- und gewerbsmäßigen*

[14] Magnetkartenlese- und Schreibgeräte können beispielsweise auf der Homepage der Firma Conrad Electronic erworben werden.

Fälschung von Zahlungskarten dar. (…) *Ob daneben der Tatbestand der Vorbereitung der Fälschung von Zahlungskarten mit Garantiefunktion gemäß § 152a Abs. 5, § 152b Abs. 5, § 149 Abs. 1 Nr. 1 StGB erfüllt ist (…), kann hier dahinstehen*“ (BGH, Urteil vom 11.08.2011, 2 StR 91/11).

Während die Frage der Strafbarkeit der verschiedenen Tatphasen hauptsächlich für die Strafverfolgungsbehörden von Bedeutung ist, wirkt sie sich auch auf die statistische Auswertbarkeit des Phänomens Skimming aus, wie im nachfolgenden Kapitel 2.3 zu sehen sein wird.

2.3 Statistische Daten

In der Polizeilichen Kriminalstatistik (PKS) für die Bundesrepublik Deutschland werden „Fälschungen von Zahlungskarten mit oder ohne Garantiefunktion, Schecks und Wechseln gemäß“ §§ 152a, 152b StGB erfasst (Schlüssel 553000). Auch Vorbereitungshandlungen im Sinne des § 149 StGB werden gelistet (Schlüssel 551000). Für das Jahr 2012 wurden 2.985 Fälle im Sinne der §§ 152a, 152b StGB erfasst, was einen Rückgang zum Vorjahr um 35 % bedeutet (2011: 4.590 erfasste Fälle). Diese Zahlen sind jedoch im Rahmen der Untersuchung nicht verwertbar, da unter den aufgezeigten Schlüsseln zahlreiche Straftaten zusammengefasst sind, nicht nur Skimming-Straftaten. So umfasst § 152b StGB beispielsweise auch die Fälschung von Euroschecks, also ein gänzlich anderes Delikt. Eine spezifische Erfassung fehlt, sodass nicht gesagt werden kann, wie viele der statistisch erfassten Fälle auf Skimming-Straftaten entfallen. Hinzu kommt, dass eine „Skimming-Straftat“ verschiedene Straftatbestände des Strafgesetzbuches verwirklichen kann, wie unter Kapitel 2.2 dargestellt.

Außerdem kann die PKS nur Straftaten abbilden, die den Polizeibehörden bekannt geworden sind und insofern nur das Hellfeld darstellen kann. Im Bereich von Skimming-Straften ist zu vermuten, dass ein Großteil der Straftaten nicht angezeigt wird – obwohl den Geldinstituten und Kreditkartenorganisationen nahezu alle Fälle bekannt sein dürften[15]. Dies hat folgenden Hintergrund: Stellt ein betroffener Bankkunde unautorisierte Buchungen fest, meldet er diese in aller Regel bei seinem kontoführenden Bankinstitut. Das je-

[15] Ausnahme: Unberechtigte Buchung bleibt durch Bankkunden und Bankinstitut unerkannt.

weilige Geldinstitut bzw. die Kreditkartenorganisation stellt einen Fall von Skimming fest, bearbeitet diesen Schadensfall intern und erstattet dem Bankkunden die verloren gegangene Summe. Somit entfällt für den Bankkunden der monetäre Beweggrund zu einer Anzeigenerstattung. Die Bankinstitute wiederum meiden Strafanzeigen, da sie Reputationsschäden fürchten (Treude 2011, S. 7). Somit kann eine Entwicklung von Skimming-Straftaten nicht durch die PKS abgebildet werden (Bundeskriminalamt 2013b, S. 217–218).

Das Bundeskriminalamt veröffentlicht in regelmäßigen Abständen Lagebilder zur Zahlungskartenkriminalität. Diese Lagebilder enthalten Angaben zur Zahl der manipulierten Geldautomaten sowie zu den sogenannten „Attacken", also den einzelnen Manipulationen. Einzelne Geldautomaten kann merfach „attackiert" werden, etwa in hoch frequentierten Bereichen, wie Fußgängerzonen (Bundeskriminalamt 2013a, S. 6). Diese Zahlen veröffentlich das Bundeskriminalamt mit dem Hinweis: „*Belastbare Gesamtzahlen zur bundesweiten Fall- und Schadensentwicklung liegen der Polizei* (…) *nicht vor. Ein Großteil der Straftaten wird nicht angezeigt, da der Schaden des Betroffenen durch die Geldinstitute und Kreditkartenorganisationen in der Regel erstattet wird. Die Informationspolitik der Kartenorganisationen und Dachverbände hinsichtlich der erlittenen Verluste und Missbrauchsumsätze ist seit Jahren sehr restriktiv*" (Bundeskriminalamt 2012, S. 6). In einer Fußnote heißt es weiter: „*Dem Bundeskriminalamt stehen keine konkreten Zahlen zur Verfügung*" (ebenda).

Grundsätzlich müssten der Firma EKS Zahlen aller bekannt gewordenen Schadensfälle durch Skimming-Straftaten vorliegen, da sie den Haftungsfonds der Kreditwirtschaft verwaltet, eingehende Schadensmeldungen prüft und die Berechtigungen zu Ausgleichszahlungen erteilt. Seitens der Firma EKS bzw. des ZDS werden jedoch keine Zahlen mehr veröffentlicht.

Im Rahmen diverser Änderungen am Bundesdatenschutzgesetzes (BDSG) im Jahr 2009[16] wurde § 42a BDSG („Informationspflicht bei unrechtmäßiger

[16] Die Änderungen sind am 01.09.2009 in Kraft getreten.

Kenntniserlangung von Daten“) eingeführt: „*Stellt eine nichtöffentliche Stelle (…) fest, dass bei ihr gespeicherte* (…) *personenbezogene Daten zu Bank- oder Kreditkartenkonten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, hat sie dies* (…) *unverzüglich der zuständigen Aufsichtsbehörde sowie den Betroffenen mitzuteilen.*“ Diese Regelung gilt auch für Bankdaten, die im Zuge von Skimming-Straftaten unrechtmäßig abgegriffen wurden. Zweck dieser Regelung ist unter anderem eine „*Präventivwirkung durch Publizität*“ (BDSG 2013, S. 955). Um Imageschäden, die durch eine Publikation entstehen könnten, zu vermeiden, sollen verstärkte Sicherheitsvorkehrungen im Vorfeld erreicht werden. Da bei Daten zu Bank- oder Kreditkartenkonten (u.a. Kontonummer, Kreditkartennummer) ein hoher Schaden eintreten könnte, gilt die Regelung auch hinsichtlich dieser Daten (vgl. BDSG 2013, S. 956). Über entsprechende Meldungen könnte eine Statistik aller Skimming-Angriffe geführt werden. Im Jahr 2013 hat das Magazin für Computertechnik, c´t, bei den Datenschutzbehörden der Länder sowie den jeweiligen Landeskriminalämtern nachgefragt, wie viele Skimming-Fälle gemeldet wurden. Das Ergebnis war ernüchternd, nur wenige Skimming-Angriffe waren gemeldet worden (vgl. Oppong 2013). Auch der frühere Bundesdatenschutzbeauftragte Peter Schaar hatte sich zur Umsetzung der Regelung kritisch geäußert: „*Die Anzahl der bundesweit gemeldeten Fälle belegt, dass die Informationspflicht bei Datenschutzpannen von den verantwortlichen Stellen ernst genommen wird. Dennoch gehe ich von einer hohen Dunkelziffer nicht gemeldeter Vorfälle aus. Häufig ist auch die Kommunikation der verantwortlichen Stellen gegenüber der Öffentlichkeit und den Datenschutzbehörden noch stark verbesserungsbedürftig“* (BfDI 2011). Insofern können auch über das BDSG keine belastbaren statistischen Zahlen in Erfahrung gebracht werden.

Die im „Bundeslagebild Zahlungskartenkriminalität“ jährlich veröffentlichten Daten lassen lassen einen Trend erkennen:

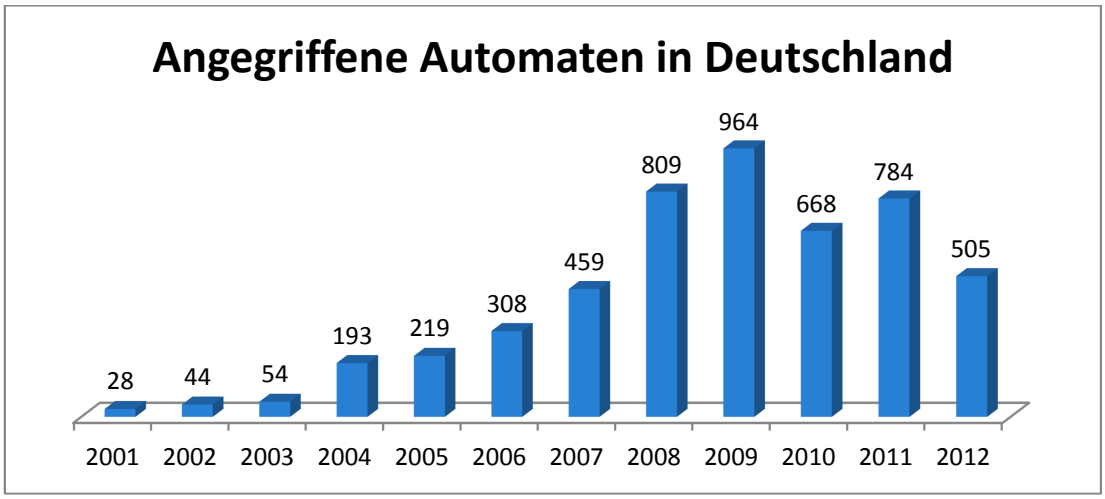


Abbildung 2: Angegriffene Automaten in Deutschland
(vgl. Bundeskriminalamt 2011, S. 6 und Bundeskriminalamt 2013, S. 6)

Nach erstmals erfassten Fällen im Jahr 2001 ist die Anzahl stetig gestiegen. In den Jahren 2008 bis 2010 wurden die meisten Geldautomaten angegriffen. Nach Erkenntnissen des Bundeskriminalamtes wurde im Jahr 2010 die höchste Zahl an Attacken registriert. Seitdem sind die Zahlen rückläufig, aber noch immer deutlich über dem Anfangsniveau. Zahlen für das Jahr 2013 lagen bei Erstellung der Arbeit noch nicht vor.

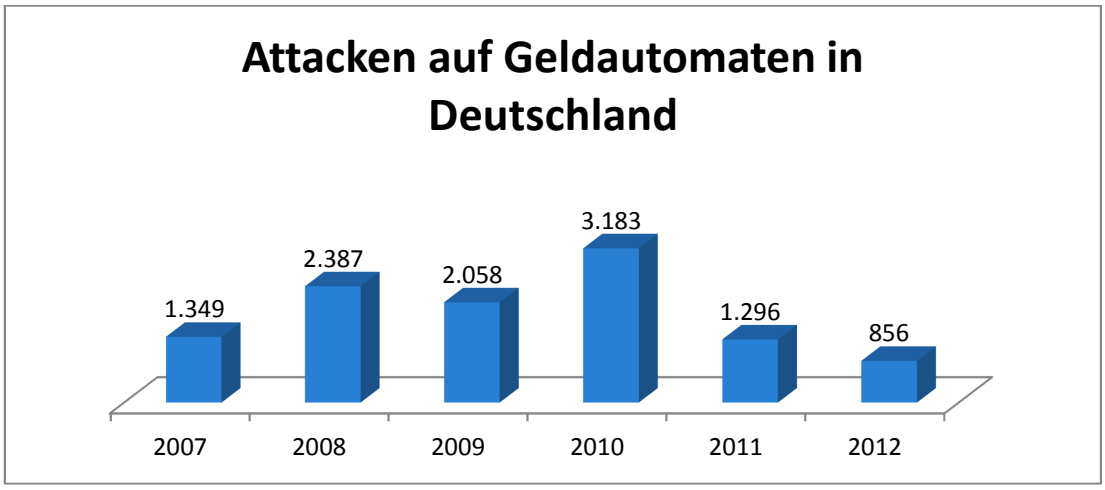


Abbildung 3: Attacken auf Geldautomaten in Deutschland
(Bundeskriminalamt 2011, 2013a)

Hinsichtlich der teils starken Schwankungen der Fallzahlen in diesem Deliktsfeld ist anzunehmen, dass diese – zumindest teilweise – auf die Einführung neuer Sicherungsmechanismen zurückzuführen sind. Durch den Einbau neuer Technik werden die Täter gezwungen ihre Tatmittel anzupassen. Das Vorgehen der Täter wird erschwert oder in Teilbereichen gar unmöglich gemacht. Die Täter reagieren zeitlich verzögert auf (sicherheits-)technische

Neuerungen: „*Erfahrungsgemäß stellen sich Täter flexibel und schnell auf veränderte Strafverfolgungsmaßnahmen und neue Sicherungsmechanismen ein*“ (Treude 2011, S. 12).

Der Rückgang seit dem Jahr 2010 ist laut Bundeskriminalamt hauptsächlich auf die Einführung der Chiptechnologie zurückzuführen (Bundeskriminalamt 2013a). Der Beitritt der USA sowie zahlreicher Länder aus dem Raum Asien/Pazifik zur sogenannten „EMV-Haftungsumkehr“ im April 2013 trägt zur Verbreitung der EMV-Technologie und somit zur Eindämmung von Schadensfällen deutscher Zahlungskarteninhaber durch Abgreifen der Magnetstreifendaten im Ausland bei (dpa-AFX Wirtschaftsnachrichten GmbH). Auch eine Studie der Europäischen Zentralbank kommt zu dem Schluss, dass die Einführung des EMV-Standards zu dem Rückgang der Fallzahlen geführt hat: „*When analysing counterfeit fraud at ATMs*[17] *and POS terminals, it can be assumed that migration to the EMV standard has contributed to a decline in the level of counterfeit card fraud acquired in SEPA countries*“[18] (Report on card fraud 2012, S. 18).

Während die Manipulationsfälle an Geldautomaten rückläufig sind, steigen die Fallzahlen für Skimming-Straftaten an POS-Terminalgeräten an. Das Bundeskriminalamt meldete für das Jahr 2012 77 vollendete Fälle sowie ca. 500 weitere Fälle, in denen POS-Terminalgeräte durch die Netzbetreiber vorsorglich ausgetauscht wurden, da ein Manipulationsverdacht vorlag. Im Jahr 2012 wurden nach Angaben des Bundeskriminalamtes rund 20.000 deutsche Zahlungskarten gesperrt, um ein mögliches Cashing zu verhindern. Unter allen Kartensperrungen, die bei deutschen Zahlungskarten vorgenommen wurden, entfielen 14 % auf vorangegangene Terminalmanipulationen bzw. Verdachtsfälle (vgl. Bundeskriminalamt 2013a, S. 7). Manipulationen an POS-Terminalgeräten zu erkennen, ist äußerst schwierig. In einigen Fällen wurde die Elektronik zum Abgreifen der Daten im Inneren des Terminalgerätes installiert (ebenda).

[17] Englisch automated/automatic teller machine - Geldautomat

[18] *Bei der Analyse von Betrugsstraftaten mittels Kartenfälschungen an Geldautomaten oder Terminalgeräten kann angenommen werden, dass die Umstellung auf den EMV-Standard zum Rückgang der Straftaten durch gefälschte Zahlungskarten im SEPA-Raum beigetragen hat.*

In einer Grafik verdeutlicht das Bundeskriminalamt die Verteilung der Cashing-Straftaten:

Abbildung 4: Haupteinsatzstaaten gefälschter Debitkarten mit deutschen Kartendaten2012
(Bundeskriminalamt 2013a)

Durchschnittlich werden pro Attacke 60 Zahlungskartendaten abgegriffen (vgl. Treude 2011, S. 7). Zuletzt schätzte das Bundeskriminalamt den Schaden, der durch den Einsatz gefälschter deutscher Debitkarten[19] entstanden ist, im Jahr 2011 auf rund 35 Millionen Euro. Im Vorjahr (2010) auf 60 Millionen Euro (vgl. Bundeskriminalamt 2012, S. 6). Für das Jahr 2012 wurden keine Angaben zu den Schadenssummen gemacht.

Die Europäische Agentur für Netz- und Informationssicherheit[20] (ENISA) bezifferte den Verlust durch Skimming-Straftaten in Europa für das Jahr 2008 auf knapp 500 Millionen Euro (484.184.901 €). Der US-Geheimdienst bezifferte den Schaden durch Geldautomatenbetrug für das Jahr 2008 allein in den USA auf 350.000 USD täglich (ENISA 2009, S. 12).

[19] Das Bundeskriminalamt machte keine Angaben zu Kreditkartenschäden.
[20] European Union Agency for Network and Information Security. 2004 von der Europäischen Union gegründete Agentur, deren Zuständigkeitsbereich u.a. die Netz- und Informationssicherheit umfasst.

Zu den Tatverdächtigen führt das Bundeskriminalamt wenig aus. Es gibt an, dass rumänische und bulgarische Tatverdächtige dominieren. Über die Staatsangehörigkeit werden keine weiteren Feststellungen getroffen (wie etwa Altersstruktur, Geschlecht, etc.). Das Vorgehen der Tätergruppierungen wird als flexibel und arbeitsteilig beschrieben (Bundeskriminalamt 2013a, S. 9). Darüber hinaus gibt es keine statistischen Angaben zu den Tätern, die PKS kann aufgrund der bereits dargelegten Aspekte nicht herangezogen werden.

2.4 Forschungsstand

In der deutschsprachigen Literatur, speziell in Zeitschriften, sind neben Beiträgen zur aktuellen Lage Abhandlungen zur strafrechtlichen Problematik zu finden. Zudem gibt es zur kriminalistischen Vorgehensweise (meist mit dem Schwerpunkt der polizeilichen Sachbearbeitung) zahlreiche Beiträge in Fachzeitschriften. In diesen Beiträgen werden überwiegend Erfahrungen der Ermittlungsbehörden dargestellt, die in Teilen auch kriminologische Erkenntnisse umfassen. Die Tatverdächtigen stammen nahezu ausschließlich aus südosteuropäischen Ländern. Deutsche Staatsangehörige bilden im Deliktsfeld Skimming die Ausnahme (Bundeskriminalamt 2013a, S. 9). Darüber hinaus ist den Aufsätzen zu entnehmen, dass es sich um „*ein typisches Bandendelikt mit arbeitsteiliger Aufgabenverteilung*“ (Schmidt 2012, S. 16) handelt. Die sogenannten „Hintermänner“ agieren meist aus Rumänien und Bulgarien. Von Festnahmen betroffen sind vorwiegend die „*Arbeiter vor Ort*“ (ebenda), die beim An-/Abbau der Skimming-Technik entdeckt werden. Bei der Manipulation sind die Täter häufig zu zweit, in manchen Fällen ist noch ein Fahrer hinzuzurechnen. „*Ausserdem* (sic!) *wurden sie meistens vor Ort von einem vierten Mann geführt, der kaum als solcher erkannt wurde*“ (Blaser und Stauffenegger 2011, S. 16).

Ein Beitrag unter dem Titel „*Skimming – Eine kriminologische Betrachtung*“ (Bachmann und Goeck 2011, S. 153) befasst sich mit der Phänomenologie des Deliktes Skimming. Die Ausführungen umfassen neben strafrechtlichen Aspekten eine kurze Darstellung der Lage sowie den Hinweis, dass die Her-

kunft der Täter Südosteuropa ist und die Vorgehensweise arbeitsteilig. Zudem wird eine mögliche Motivlage angerissen: Die Autoren verweisen auf eine Urteilsbegründung des Bundesgerichtshofes: „*Auch das Tatinteresse der Angeklagten war hoch; denn der Umfang der ihnen zum Teil gezahlten und im Übrigen versprochenen Entlohnung mag zwar nach herkömmlichen mitteleuropäischen Maßstäben eher gering erscheinen; das Entgelt hätte den Angeklagten jedoch in ihrer Heimat für mehrere Monate zum Leben genügt*“ (BGH, Urteil vom 27.02.2011, 3 StR 419/10).

Den Blick auf internationale Veröffentlichungen weitend, führt zu einer Ausarbeitung von Michael Levi aus dem Jahr 2008. Levi hat bis dahin erschienene Literatur zur Thematik „organisierter Betrug“ ausgewertet und zusammengefasst. Levi kommt zu dem Schluss: „*Eastern Europeans have devloped a reputation for technical skill and cross-border operations*” (Levi, S. 410). Er ergänzt: “*Rumanians also have played a significant role in the use in the UK of technical devices on ATMs* (…) *to capture payment card PINs*”[21] (Levi, S. 410–411).

Levi stellt zudem zwei Merkmale heraus, um zwischen einer lose zusammengehaltenen Bande von Betrugsstraftätern[22] und einer hierarchischen Organisation zu unterscheiden. Zum einen betrachtet er, ob sich die Suche von Mittätern für die einzelnen Arbeitsschritte einfach oder schwer gestaltet. Zum anderen betrachtet er die Arbeitsteilung einer Bande: Je feingliedriger, desto besser müsse die Organisation funktionieren. Er umschreibt diese zwei Merkmale mit den Begriffen Netzwerk und Drehbuch (vgl. Levi, S. 390).

Zur Motivation bzw. als Erklärung von Cybercrime[23] führt Levi aus: „*cyber-fraud techniques reflect a comparative criminal advantage arising from the*

[21] *Osteuropäer haben sich einen Ruf für technische Fähigkeiten und grenzübergreifende Tätigkeiten erarbeitet. Rumänen spielen eine signifikante Rolle beim Einsatz von technischen Zusatzgeräten an Geldautomaten im Vereinigten Königreich Großbritanniens und Nordirlands.*

[22] Unter dem Begriff „fraud“ (englisch fraud – Betrug) fasst Levi diverse Straftaten zusammen, so auch Skimming.

[23] Englisch Cybercrime – Internetkriminalität. Während der Begriff Internetkriminalität in Deutschland nur selten mit Skimming in Verbindung gebracht wird (Skimming-Täter nutzen das Internet lediglich für den Austausch abgegriffener Daten und zu Kommunikationszwecken), werden Skimming-Straftaten im internationalen Sprachgebrauch unter den Oberbegriff Cybercrime subsumiert.

combination of high technological skills and high motivation because of poor opportunities in their home countries“[24] (Levi, S. 396).

Die Auswertung der aktuell existierenden Literatur zeigt, dass der derzeitige Forschungsstand keine Antwort auf die forschungsleitende Frage geben kann.

3. Die Täter im Blickfeld: Empirie

Eine offen verfasste Fragestellung, wie in diesem Fall die forschungsleitende Frage, benötigt eine explorativ angelegte Methodik mit überwiegend qualitativen Erhebungsinstrumenten. Zu Beginn der Untersuchung stand die qualitativ-quantitative Inhaltsanalyse von Ermittlungsakten. Daran schloss die qualitative Befragung von Experten – Personen, die auf Seiten der Strafverfolgung regelmäßig und seit einem längeren Zeitraum mit der Bearbeitung von Skimming-Straftaten befasst sind – mittels schriftlichem Fragebogen an. Den Abschluss bildete das qualitative Interview eines rechtskräftig verurteilten Skimming-Straftäters. Somit wurden „*unterschiedliche Perspektiven auf einen untersuchten Gegenstand*“ (Flick 2011, S. 12) eingenommen. Im Verlauf der Untersuchung wurden verschiedene Methoden miteinander kombiniert, um deren jeweilige Reaktivität zu begrenzen (vgl. Flick 2011, S. 15). Letztlich soll dies der Erkenntniserweiterung und dem umfassenderen Blick auf den Untersuchungsgegenstand dienen. So geben die Ermittlungsakten (weitgehend) ermittelte Tatsachen wieder, die Experten geben ihre Erfahrungen und Eindrücke aus Sicht eines Beobachters wieder und der Insasse schildert seine Wahrnehmungen aus der Perspektive des Täters. Insofern sind die einzelnen Erhebungsinstrumente in Ergänzung zueinander angewandt worden.

3.1 Inhaltsanalyse von Ermittlungsakten

Eingangs wurde eine quantitativ-qualitative Inhaltsanalyse von Ermittlungsakten vorgenommen. Ermittlungsakten bestehen aus diversen schriftlichen Dokumenten, denen eine Vielzahl von Daten entnommen werden kann. Durch das Extrahieren bestimmter, vorher festgelegter, Angaben aus den jeweiligen

[24] *Cybercrime hat einen vergleichsweise kriminellen Vorteil, der in der Kombination von hoch technologischen Fertigkeiten und hoher Motivation begründet ist, in Anbetracht der schlechten Bedingungen in den Heimatländern.*

Akten wurde eine Informationsbasis geschaffen, die sich von den ursprünglichen Dokumenten unterscheidet und lediglich die für die forschungsleitende Frage wichtigen Informationen enthält (Gläser und Laudel 2010, S. 199–200).

3.1.1 Feldzugang, Erhebung der Daten und Methodik

Für die Inhaltsanalyse von Ermittlungsakten wurde bei der Staatsanwaltschaft (StA) Frankfurt a.M. Akteneinsicht für ein wissenschaftliches Vorhaben gestellt. Dem Antrag auf Akteneinsicht wurde stattgegeben.

Der Zeitraum der Ermittlungsverfahren umfasste dabei die Jahre 2007 bis 2012. In diesem Zeitraum wurden 161 Ermittlungsverfahren wegen des Tatverdachts einer Skimming-Straftat[25] im Zuständigkeitsbereich Frankfurt a.M. geführt. Hierunter fallen versuchte oder vollendete Manipulationen von Geldautomaten. Die Anzahl der Verwertungstaten (Cashing im Ausland; Computerbetrug gemäß § 263 a StGB) ist hiervon nicht erfasst. In einem Skimming-Fall können Bankdaten diverser Bankkunden abgegriffen und missbräuchlich eingesetzt sein, sodass eine x-fache Zahl an Betrugsstraftaten begangen wird. In dieser Statistik tauchen ebenfalls keine Diebstähle von Geldautomatenteilen (z.B. Türzugangsgeräte; Teile des Karteneinzugsschachtes; Sichtblenden) auf. Diese Taten werden seitens der Ermittlungsbehörden als Vorbereitungshandlung für künftige Skimming-Straftaten („Materialbeschaffung) gesehen. Von 161 Ermittlungsverfahren richteten sich zum Zeitpunkt der Auswertung 47 Verfahren gegen einen oder mehrere namentlich bekannte Tatverdächtige. In den anderen Verfahren konnte bislang kein Tatverdächtiger ermittelt werden. Nicht alle 47 Verfahren waren für die angedachte Auswertung brauchbar. Verschiedene Ermittlungsergebnisse führten zur Eintragung eines Tatverdächtigen. In einigen Fällen kam es zu einem sogenannten „DNA-Treffer“: Am Tatort bzw. an sichergestellten Skimming-Utensilien wurde eine DNA-Spur gesichert. Ein Abgleich dieser Spur mit der DNA-Analysedatei des Bundeskriminalamtes[26] zeigte die Übereinstimmung mit dem DNA-Identifizierungsmuster einer bereits polizeilich in Erscheinung getretenen und erkennungsdienstlich behandelten Person. Diese Person war

[25] Verfahren nach § 202a Abs. 1 StGB oder § 152b Abs. 1 StGB eingetragen

[26] Eine gemäß § 81g Abs. 5 StPO beim Bundeskriminalamt geführte Datenbank, auf die alle deutschen Polizeibehörden Zugriff haben, zur Speicherung und zum Abgleich von DNA-Identifizierungsmustern.

für die Ermittlungsbehörden noch nicht greifbar, lediglich namentlich bekannt. Diese Akten enthielten über Angaben zu Namen, Geburtsdatum und Staatsangehörigkeit keine weiteren Informationen zu dieser Person oder Aussagen von dieser Person. Dagegen zeigten sich bei Festnahme eines Tatverdächtigen verschiedene, im Hinblick auf die forschungsleitende Frage auszuwertende, Aktenbestandteile. 16 Ermittlungsakten erfüllten das Kriterium „Festnahme eines Tatverdächtigen“. 13 Akten konnten zur Auswertung in den Räumlichkeiten der Justizbehörden bereit gestellt werden.

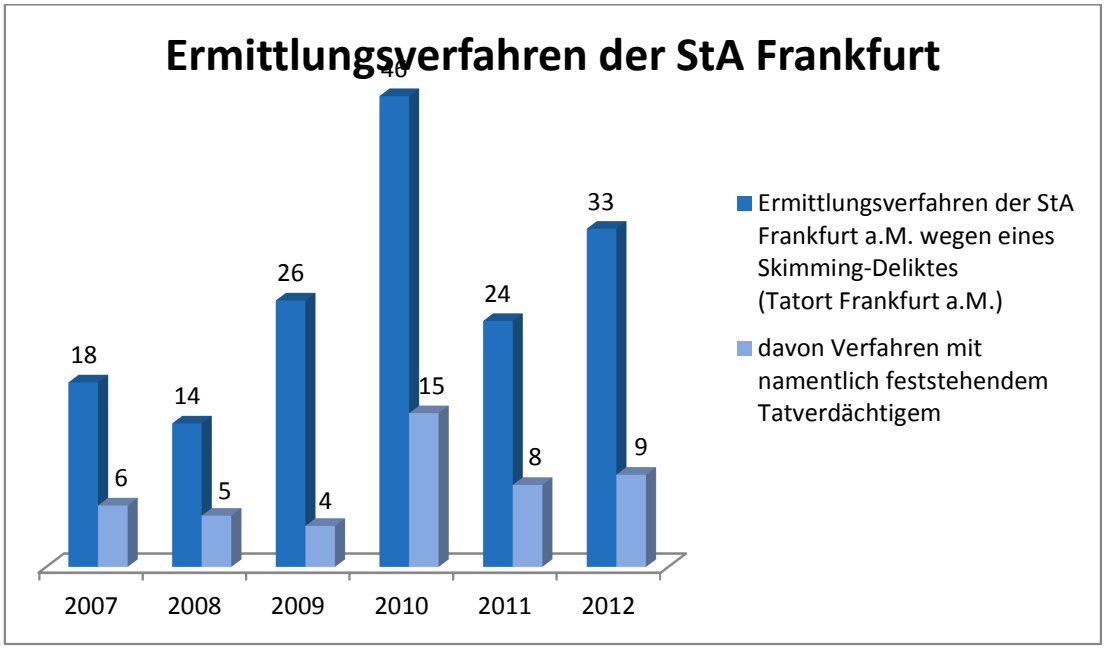


Abbildung 5: **Anzahl der Ermittlungsverfahren wegen Skimming-Straftaten im Zuständigkeitsbereich der StA Frankfurt a.M.**
Eigene Statistik durch Auszählung der Ermittlungsakten

Drei weitere Ermittlungsakten standen nicht zur Verfügung. In einem Fall war das Verfahren an eine andere Staatsanwaltschaft abgegeben worden, in zwei weitere Fällen waren die Akten nicht entbehrlich. Die bereitgestellten Akten wurden gesichtet und nach einem weiteren Kriterium ausgewählt: Akten, die kaum biografische Angaben und keine Aussage des Tatverdächtigen enthielten, wurden ausgesondert. Letztlich wurden sieben Akten ausgewählt, die sich auf neun Tatverdächtige beziehen. Gegen alle neun Personen war die Untersuchungshaft angeordnet worden. Konkreter Gegenstand der sodann erfolgten Analyse waren Beschuldigtenvernehmungen, Ermittlungsberichte der Polizei, Auszüge aus dem Bundeszentralregister, Anklageschriften,

Protokolle zur Hauptverhandlung und Urteilsbegründungen. Um aus allen Akten die gleichen Informationen erheben zu können, wurde ein einheitlicher Erhebungsbogen erstellt und die einzelnen Dokumente der Ermittlungsakten wurden hinsichtlich dieser Informationen durchsucht[27]. Nach dem Lesen der ersten drei Ermittlungsakten wurde der Erhebungsbogen nochmals modifiziert. Die aus den Texten extrahierten Daten wurden später analysiert.
Um sowohl eine Anonymisierung, als auch eine Wiedererkennung einzelner Personen im Rahmen der Auswertung zu ermöglichen, wurden sowohl die Fälle, als auch die Personen durchnummeriert und mit beispielsweise „Fall 1"/„Täter 1" bezeichnet.

3.1.2 Falldarstellungen

Im Folgenden werden die einzelnen Fälle kurz aus kriminologischer Sicht skizziert:

Fall 1, Täter 1	
Strafrechtliche Einordnung:	§§ 242, 303, 263a, 263, 152b, 152a, 25, 52, 53, 54, 74 StGB
Tatzeit:	Dezember 2009 – April 2010
Verfahrensausgang:	Freiheitsstrafe, 4 Jahre
Finanzieller Schaden (Cashing):	ca. 32.211 €
Zum Täter:	Geboren 1978 Männlich Rumänischer Staatsangehöriger Geschieden, keine Kinder Abitur/Fachhochschule Ohne erlernten Beruf

Sachverhalt

Durch ein Testkartenmonitoring des Geldinstitutes wurde der Einsatz einer Testkarte festgestellt und von einem Mitarbeiter des Geldinstitutes an den Kriminaldauerdienst gemeldet. Die eingesetzten Kriminalbeamten nahmen den Geldautomaten in Augenschein und entdeckten angebrachtes Skimming-Equipment. Daraufhin suchten sie das Umfeld nach infrage kommenden Tätern ab. In unmittelbarer Nähe zur Tatörtlichkeit wurden die Beamten auf Täter 1 aufmerksam. Dieser hatte im Außenbereich eines Cafés mit Blick

[27] Übersicht der Aktenzeichen und Erhebungskriterien, Seite 87 und Seite 87.

auf das Geldinstitut gesessen. Die Kriminalbeamten wollten Täter 1 kontrollieren. Dieser versucht jedoch zu flüchten und sich weiterer Skimming-Technik zu entledigen. Beides misslang. Im Rahmen einer Beschuldigtenvernehmung räumte der der Täter 1 den Tatvorwurf ein. Am Folgetag wurde die Untersuchungshaft angeordnet.
Im Rahmen der weiteren Ermittlungen konnten der Person mittels Videoüberwachungsbildern vorheriger Tatorte weitere Straftaten zugeordnet werden. In einigen dieser Fälle wurden die abgegriffenen Bankdaten zwischenzeitlich zum Cashing eingesetzt.

Zur Person

Täter 1, rumänischer Staatsbürger, war zum Tatzeitpunkt 32 Jahre alt und noch nicht polizeilich in Erscheinung getreten (kein Eintrag im Bundeszentralregister, keine polizeilichen Erkenntnisse).
Eigenen Angaben nach sei er in Rumänien aufgewachsen und habe dort zwölf Jahre lang die Schule besucht und diese mit dem Abitur abgeschlossen. Danach habe er Militärdienst geleistet und anschließend als selbstständiger Keramiktechniker im Betrieb der Eltern gearbeitet. Mit 22 Jahren habe er geheiratet, seine Ehefrau habe sich zwischenzeitlich von ihm getrennt. Grund hierfür sei die psychische Erkrankung seiner Mutter im Jahr 2003 und damit einhergehende Schwierigkeiten im Familienleben gewesen. Täter 1 habe auch den kleinen Keramikbetrieb aufgeben müssen, da er sich nicht gegen die wachsende Konkurrenz habe behaupten können. Seine Mutter habe nach einem stationären Aufenthalt in einer Psychiatrie weiterhin Medikamente benötigt. Die Kosten von umgerechnet etwa 70 € im Monat hätten seine Eltern von ihrer Rente in Höhe von umgerechnet etwa 200 € nicht bezahlen können. Insofern sei er auf der Suche nach Arbeit im Jahre 2004 nach Spanien gegangen. Dort habe er etwa drei Jahre in der Baubranche gearbeitet, bis sich die Immobilienkrise zugespitzt und er seine Arbeit verloren habe. Nach diversen weiteren Gelegenheitsjobs habe er sich entschlossen, in Deutschland Arbeit zu suchen.

Zur Tat/zu den Taten

Im Sommer 2009 sei der Täter 1 nach Hamburg gekommen. Dort habe er anfangs bei einem Bekannten gewohnt, welcher ihm auch für kurze Zeit Arbeit vermittelt habe. Nachdem dieser Bekannte nach Rumänien zurückgekehrt sei, habe der Täter 1 wiederum keine Arbeit gehabt. In einer Bar in Hamburg sei er mit einem Mann aus Bulgarien sowie einem Mann aus Rumänien in Kontakt gekommen. Diese beiden hätten ihn auf ein Getränk eingeladen und ihm eine lukrative Tätigkeit angeboten. Auf Nachfrage hin hätte man ihm gesagt, dass es um „Skimming" gehe. Der Verurteilte habe sich bereit erklärt und so sei es im August 2009 in Frankfurt a.M. zu einem Testlauf gekommen. Der Mann aus Bulgarien habe dem Täter 1 erklärt, was er zu tun habe. Gemeinsam seien sie in die Filiale gegangen, um die Skimming-Technik anzubringen. Wenig später habe ihn der Mann aus Bulgarien allerdings angerufen und mitgeteilt, dass der Testlauf nicht funktioniert habe, da die Polizei gekommen sei. Er werde sich wieder melden. Mitte Dezember habe man ein weiteres Treffen in Frankfurt a.M. vereinbart. An dieses Treffen hätten sich die ermittelten Skimming-Straftaten angeschlossen. Dem Täter 1 seien dabei pro Manipulation 250 € bis 300 € zugesichert worden. In allen Fällen habe der Täter 1 das benötigte Equipment von dem Mann aus Bulgarien erhalten und wieder an diesen zurückgegeben. Für vier Manipulationen habe er insgesamt 800 € erhalten. In einem weiteren Fall habe er ein Originalteil eines Geldautomaten demontiert und an den Mann aus Bulgarien übergeben. Danach sei es zur Festnahme gekommen.

Anmerkung

Die Glaubhaftigkeit der persönlichen Angaben des Täter 1 wurde seitens des Gerichts nicht angezweifelt. Die Angaben zum Tatablauf konnten durch die Beweisaufnahme umfänglich bestätigt werden.

Fall 2, Täter 2	
Strafrechtliche Einordnung:	§§ 152b, 152a, 149, 12, 22, 23, 52 StGB
Tatzeit:	Juni 2010
Verfahrensausgang:	Freiheitsstrafe, 1 Jahr und 6 Monate; Strafaussetzung zur Bewährung nach weiterem, einschlägigen Urteil widerrufen

Finanzieller Schaden (Cashing):	0 €
Zum Täter:	Geboren 1967 Männlich Rumänischer Staatsangehöriger Verheiratet, sechs Kinder Lehrabschluss Kraftfahrer

Sachverhalt

Durch ein Testkartenmonitoring des Geldinstitutes wurde der Einsatz einer Testkarte bemerkt und dem Kriminaldauerdienst gemeldet. Die eingesetzten Kriminalbeamten fanden einen manipulierten Geldautomaten vor und observierten den Foyer-Raum des Geldinstitutes. Täter 2 konnte bei der Demontage der Skimming-Geräte beobachtet und anschließend festgenommen werden. Im Rahmen einer Beschuldigtenvernehmung zeigte sich der Täter 2 geständig und räumte eine weitere Tat in einer Nachbarstadt ein. Im Rahmen einer Überprüfung dieses Geldautomaten konnte ebenfalls Skimming-Equipment sichergestellt werden. Am Folgetag wurde die Untersuchungshaft angeordnet.

Zur Person

Täter 2, rumänischer Staatsangehöriger, war zum Tatzeitpunkt 42 Jahre alt. Im Bundeszentralregister gab es zu diesem Zeitpunkt keinen Eintrag. Im Schengener Informationssystem[28] bestand ein Suchvermerk aus Italien. Dort war er als Mitglied einer Bande eingestuft, der die Fälschung von Zahlungskarten vorgeworfen wurde. Im Jahr 2008 war er in Italien zu einer sechsmonatigen Haftstrafe verurteilt worden.

Eigenen Angaben nach sei Täter 2 in Rumänien aufgewachsen und habe dort eine Lehre zum Kraftfahrer gemacht. Danach habe er in Italien einige Jahre als Fahrer gearbeitet und so seine Ehefrau und die sechs gemeinsamen Kinder unterstützt. Seine Ehefrau habe in Rumänien einen kleinen Lebensmittelhandel betrieben, welcher jedoch bereits seit Längerem keinen Gewinn abwerfe. Mit Beginn der Wirtschaftskrise habe er sein Fuhrgeschäft

[28] Das Schengener Informationssystem (SIS) ist ein Personen- und Sachfahndungssystem, das den Polizei- und Grenzschutzbehörden innerhalb der Europäischen Union automatisierte Abfragen ermöglicht. Angeschlossen sind alle EU-Mitgliedsstaaten außer dem Vereinigten Königreich, Irland und Zypern. Die Länder Island, Norwegen und Schweiz nehmen ebenfalls teil.

aufgeben müssen. Seitdem betreibe er Personenbeförderungen mit einem Minibus.

Zur Tat/zu den Taten

Täter 2 gab darüber hinaus an, im Frühjahr 2010 in Amsterdam mit einem Mann aus Rumänien ins Gespräch gekommen zu sein. Man habe über „Skimming“ gesprochen und er habe sich bereit erklärt, für 10-15 % Beteiligung an den Geldabhebungen Vorsatzgeräte an deutschen Geldautomaten zu installieren. Daraufhin habe er die Technik bekommen und sei nach Frankfurt a.M. gefahren. Dort habe er die beiden Geldautomaten manipuliert und sei im Zuge dessen in Frankfurt a.M. festgenommen worden.

Anmerkung

Die Glaubhaftigkeit der persönlichen Angaben des Täters 2 wurde seitens des Gerichts nicht angezweifelt. Die Angaben zum Tatablauf konnten durch die Beweisaufnahme bestätigt werden. Allerdings bestand der Verdacht weiterer Straftaten. Die beim Täter 2 sichergestellten Testkarten waren an weiteren Tatorten eingesetzt worden. Nähere Ermittlungsergebnisse hierzu lagen bis zur Hauptverhandlung nicht vor.

Fall 3, Täter 3	
Strafrechtliche Einordnung:	§§ 25, 30, 150, 152a, 152b StGB
Tatzeit:	August 2011
Verfahrensausgang:	Einstellung gemäß § 154 I StPO unter Hinweis auf weiteres anhängiges Verfahren
Finanzieller Schaden (Cashing):	0 €
Zum Täter:	Geboren 1988 Männlich Rumänischer Staatsangehöriger Ledig, keine Kinder Grund-/Hauptschule Ohne erlernten Beruf

Sachverhalt

Im Rahmen von Hotelkontrollen fiel die Ähnlichkeit einer angetroffenen Person, des Täters 3, zu Fahndungsbildern wegen einer Geldautomaten-

Manipulation auf. Die Durchsuchung des Hotelzimmers führte zum Auffinden diverser Skimming-Utensilien. Eine Überprüfung infrage kommender Bankfilialen deckte eine aktuelle Manipulation auf. Für das Hotelzimmer waren zwei weitere Personen eingecheckt, welche zum Zeitpunkt der Kontrolle nicht vor Ort waren. Die Überwachungsbilder des betroffenen Geldinstituts zeigten drei Männer bei der Tatausführung. Im Rahmen der Personenkontrolle des Täters 3 konnte eine gefälschte Kreditkarte aufgefunden werden. Im Rahmen einer Vernehmung räumte der Täter 3 den Tatvorwurf ein und wies auf eine weitere Manipulation hin. Diese Manipulation war durch einen aufmerksamen Bankkunden entdeckt worden, die eingesetzte Technik war bereits sichergestellt worden. Noch am gleichen Tag wurde die Untersuchungshaft angeordnet.

Zur Person

Täter 3, rumänischer Staatsangehöriger, war zum Tatzeitpunkt 23 Jahre alt. Über die beiden Taten hinaus war er polizeilich nicht in Erscheinung getreten, im Bundeszentralregister gab es keinen Eintrag.

Zur Tat/zu den Taten

Täter 3 hatte im Rahmen der Vernehmung angegeben, drei Tage vor der Tat mit dem Auto eingereist zu sein. Mit ihm seien zwei weitere Männer aus Rumänien gekommen, wovon einer mit ihm in Frankfurt geblieben sei. Gemeinsam mit einer unbekannten dritten Person habe man Geldautomaten manipulieren wollen. Er habe die Vorrichtungen abnehmen und in das Hotel bringen sollen. Die Geräte habe der zweite Mann aus Rumänien bekommen, dieser habe auch einen Laptop. Täter 3 wisse nicht, von wem seine Begleitung die Geräte bekommen habe. Den Mann aus Rumänien habe er in einem Lokal in seiner Heimatstadt kennengelernt. Die Bezahlung hätte nach zwei bis drei Wochen durch die unbekannte dritte Person erfolgen sollen.

Gegen den Täter 3 sowie gegen die dritte (für den Täter 3 unbekannte) Person, die ebenfalls in dem Zimmer wohnte, wurde zeitgleich in einem umfangreichen Verfahren der Staatsanwaltschaft Baden-Baden ermittelt. Auf dem in Frankfurt sichergestellten Skimming-Equipment befanden sich Kartendaten, die bei Tatorten in Baden-Württemberg abgegriffen wurden. Zudem führte ein

Abgleich eines DNA-Abriebes der sichergestellten Skimming-Technik mit der DNA-Analyse-Datei zu einem Personentreffer. Spurenverursacher war ein weiterer rumänischer Staatsangehöriger, der aus der gleichen Stadt stammt, wie der Täter 3 und zum Zeitpunkt der Tat in der Justizvollzugsanstalt Brandenburg einsaß (Verabredung zur Fälschung von Zahlungskarten mit Garantiefunktion, Staatsanwaltschaft Potsdam).

Anmerkung
Ohne.

Fall 4, Täter 4	
Strafrechtliche Einordnung:	§§ 152b, 152a, 263a, 27, 52, 56 StGB
Tatzeit:	Oktober – November 2012
Verfahrensausgang:	Freiheitsstrafe, 1 Jahr und 6 Monate; Strafaussetzung zur Bewährung
Finanzieller Schaden (Cashing):	Ca. 10.000 €
Zum Täter:	Geboren 1982 Männlich Bulgarischer Staatsangehöriger Ledig, keine Kinder Lehrabschluss Skilehrer, Monteur

Sachverhalt:
Aufgrund einer Skimming-Serie wurden diverse Bankfilialen durch die Kriminalpolizei überwacht. Im Zuge der polizeilichen Maßnahmen konnten zwei Täter „auf frischer Tat" festgenommen werden (siehe Fall 5, Täter 5). Die Untersuchungshaft wurde angeordnet.

Zur Person
Täter 4, bulgarischer Staatsangehöriger, war zum Tatzeitpunkt 30 Jahre alt und noch nicht polizeilich in Erscheinung getreten (kein Eintrag im Bundeszentralregister, keine polizeilichen Erkenntnisse).
Täter 4 arbeitete eigenen Angaben zu Folge in den Wintermonaten als Skilehrer und in den Sommermonaten als Monteur. Er sei ledig gewesen und habe keine Kinder gehabt.

Zur Tat/zu den Taten

Um eine Augenoperation für seinen Großvater finanzieren zu können, habe er sich über einen Freund umgerechnet etwa 3.000 € von einer ihm unbekannten Person geliehen. Dabei sei er von einem normalen Kredit ausgegangen. Später schlug man ihm vor, in Frankfurt a.M. Skimming-Technik an Bankautomaten anzubringen, um den Kredit zu tilgen. Da er angewiesen worden sei, einen weiteren Mann mit nach Deutschland zu nehmen, habe er seinen langjährigen Bekannten, den Täter 5 (gleicher Wohn- und Geburtsort), angesprochen. Gemeinsam sei man einige Tage vor der Festnahme mit dem Bus nach Frankfurt gereist. Nach einem Anruf aus Bulgarien habe man von Unbekannten die entsprechenden Geräte erhalten, zudem auch die Anweisung, Geldautomaten eines bestimmten Geldinstitutes auszuwählen. Mittels eines Computerprogramms auf einem mitgeführten Laptop habe man die Kartendaten an die bulgarischen Hintermänner übermittelt, die PIN-Nummern via Skype[29]. Pro Datensatz habe man ihnen zusammen 50 $ versprochen (= 25 $ pro Person). Bis zum Zeitpunkt der Festnahme habe man lediglich per Western Union Geld[30] für die Auslagen (Hotelkosten, Verpflegung) erhalten.

Anmerkung

Die Glaubhaftigkeit der persönlichen Angaben des Täters 4 wurde seitens des Gerichts nicht angezweifelt. Die Angaben zum Tatablauf deckten sich weitgehend mit den Angaben des Täters 5 und konnten durch die weitere Beweisaufnahme größtenteils bestätigt werden. Allerdings lagen digitalforensische Untersuchungsergebnisse (Auswertung der sichergestellten Skimming-Technik sowie der sichergestellten Hardware) bis zur Hauptverhandlung nicht vor.

Fall 5, Täter 5	
Strafrechtliche Einordnung:	§§ 152b, 152a, 263a, 27, 52, 56 StGB
Tatzeit:	Oktober – November 2012

[29] Software der Firma Microsoft Corporation, die das kostenlose Telefonieren zwischen Skype-Kunden über das Internet ermöglicht.

[30] Die Firma Western Union AG ermöglicht einen weltweiten Transfer von Bargeld. Zahlt eine Person in einer Filiale einen Geldbetrag ein, erhält sie hierzu eine Referenznummer. Der Empfänger kann sich das eingezahlte Geld unter Vorlage dieser Referenznummer an einer anderen Filiale auszahlen lassen.

Verfahrensausgang:	Freiheitsstrafe, 1 Jahr und 6 Monate; Strafaussetzung zur Bewährung
Finanzieller Schaden (Cashing):	Ca. 10.000 €
Zum Täter:	Geboren 1963 Männlich Bulgarischer Staatsangehöriger Verheiratet, zwei Kinder Lehrabschluss Skilehrer, Schlosser

Sachverhalt

Aufgrund einer Skimming-Serie wurden diverse Bankfilialen durch die Kriminalpolizei überwacht. Im Zuge der polizeilichen Maßnahmen konnten zwei Beschuldigte „auf frischer Tat" festgenommen werden (siehe Fall 4, Täter 4). Die Untersuchungshaft wurde angeordnet.

Zur Person

Täter 5 bulgarischer Staatsangehöriger, war zum Tatzeitpunkt 47 Jahre alt und noch nicht polizeilich in Erscheinung getreten (kein Eintrag im Bundeszentralregister, keine polizeilichen Erkenntnisse).

Täter 5 war eigenen Angaben zu Folge verheiratet und lebte mit seiner Frau und den beiden gemeinsamen Kindern. Ein Sohn sei bereits erwachsen gewesen und habe zu diesem Zeitpunkt die Familie ernährt, indem er Grundstücke bewirtschaftete. Täter 5 sei von Beruf Schlosser und Skilehrer. Eine Arbeit habe er jedoch nur in den Wintermonaten als Skilehrer und teilweise als Skiliftarbeiter.

Zur Tat/zu den Taten

Da Täter 5 nur umgerechnet etwa 300 € im Monat zur Verfügung gehabt habe, sei er auf den Vorschlag seines Bekannten, Täter 4, eingegangen, zum Skimming nach Deutschland zu fahren. Dies habe er in einem Café im gemeinsamen Wohnort besprochen. Ihm seien für jede Bankkarte 50 $ versprochen worden. Die Geräte hätte der Täter 4 von einer ihm unbekannten dritten Person bekommen. Man sei erst nach Mailand geflogen und dann mit dem Bus weiter gereist. Vor Ort habe man Anrufe aus Bulgarien mit genauen Anweisungen bekommen. In den ersten Tagen seien er und Täter 4 auf der Suche nach Geldautomaten gewesen, die den Beschreibungen aus Bulgari-

en entsprochen hätten. Wobei man die konkrete Anweisung bekommen habe, nur Geldautomaten eines bestimmten Geldinstitutes aufzusuchen. Die Kartendaten habe man nach dem Skimming über das Notebook, welches man zu diesem Zweck in Bulgarien erhalten habe, an den unbekannten Dritten übermittelt. Die dazugehörigen persönlichen Identifikationsnummern über Skype. Die Skimming-Geräte habe man erst in Frankfurt erhalten. Die unbekannte Person habe sie aus Bulgarien angerufen und ihnen einen Treffpunkt genannt. Dort habe ihnen eine weitere unbekannte Person – er vermute ebenfalls ein Mann aus Bulgarien – die Technik übergeben. Über Western Union bekäme man zudem Geld „zum Leben".

Anmerkung

Die Glaubhaftigkeit der persönlichen Angaben des Verurteilten wurde seitens des Gerichts nicht angezweifelt. Die Angaben zum Tatablauf deckten sich weitgehend mit den Angaben des Mittäters (siehe Fall 4) und konnten durch die weitere Beweisaufnahme größtenteils bestätigt werden. Allerdings lagen digitalforensische Untersuchungsergebnisse (Auswertung der sichergestellten Skimming-Technik sowie der sichergestellten Hardware) bis zur Hauptverhandlung nicht vor.

Fall 6, Täter 6	
Strafrechtliche Einordnung:	§§ 149, 152b, 303b, 22, 23, 25, 52 StGB, §§ 1, 105 JGG
Tatzeit:	April 2007
Verfahrensausgang:	Verwarnung, Dauerarrest von 4 Wochen
Finanzieller Schaden (Cashing):	0 €
Zum Täter:	Geboren 1986 Rumänischer Staatsangehöriger Männlich Ledig, keine Kinder Abitur/Fachhochschule Student (Informatik)

Sachverhalt

Aufgrund des Alarms eines Anti-Skimming-Moduls kontrollierten Polizeibeamte einen Geldautomaten, stellten die Manipulation mittels Skimming-Technik fest und kontrollierten im Nahbereich des Geldautomaten zwei ver-

dächtige Personen (siehe Fall 7a, Täter 7). Im Rahmen der körperlichen Durchsuchung der Täter 6 und 7 wurden Skimming-Utensilien aufgefunden. Gegen beide Täter wurde Untersuchungshaft angeordnet.

Zur Person

Täter 6, rumänischer Staatsangehöriger, war zum Tatzeitpunkt 21 Jahre alt und noch nicht polizeilich in Erscheinung getreten (kein Eintrag im Bundeszentralregister, keine polizeilichen Erkenntnisse).

Täter 6 war eigenen Angaben zu Folge zum Tatzeitpunkt ledig und verfügte über ein monatliches Einkommen von umgerechnet etwa 100 €. Hierbei handele es sich um ein Stipendium für sein Studium der Informationstechnik (2. Studienjahr). Dieses Stipendium habe er aufgrund guter Leistungen erhalten. Im Alter von 18 Jahren sei seine Mutter verstorben. In diesem Monat habe er sein Abitur gemacht. Anschließend habe er noch weitere Prüfungen absolviert, um das Studium beginnen zu können. Bei seinem Vater lebe er seit Längerem nicht mehr, da dieser alkoholkrank sei. Er habe bei Verwandten gewohnt. Eigentlich wolle er mit seiner Freundin zusammenziehen, dazu fehle das nötige Geld. Die Freundin war bei der Hauptverhandlung anwesend.

Täter 6 gab zudem im Rahmen seiner Beschuldigtenvernehmung an, ehrenamtliche Hilfe für Angehörige krebskranker Menschen zu leisten. Dies werde über die örtliche Kirche organisiert.

Aus der Untersuchungshaft heraus schrieb der Täter 6 einen Brief an das Gericht. In diesem Brief schilderte er sein bisheriges Leben und welchen Einfluss die Alkoholkrankheit seines Vaters aber auch die Hilfe seiner Freundin auf ihn hatten.

Zur Tat/zu den Taten

Im April 2007 sei der Täter 6 mit dem Bus nach Deutschland gereist, um hier für zwei Monate einer Arbeit nachzugehen, bevor das nächste Semester beginne. Im Bus habe er den Täter 7 kennengelernt. Dieser habe ihm umgerechnet zwischen 5.000 € und 10.000 € für die Montage von Geräten an Geldautomaten versprochen. Davon habe er zuvor noch nichts gehört. Beeindruckt von dem hohen, versprochenen Ertrag sowie der Aussage des Täters 7, man müsse dabei keine Gewalt anwenden und es bestünden keine

Risiken, habe er mitgemacht. Bei der Tat habe man sich die beiden Geräte aufgeteilt. Er habe „das große Teil“ anbringen müssen, während der Täter 7 „das kleine Teil“ angebracht habe. Täter 7 habe ihm auch eine Übernachtungsmöglichkeit in einer Stadt in der Nähe von Frankfurt besorgt. Dort hätten neben der Frau des Täters 7 und dem gemeinsamen Kind weitere Bekannte des anderen Täters gewohnt. Die Geräte hätte der Täter 7 von einem Spanier bekommen und hätte sie nach dem Skimming auch an diesen zurückgeben. Nach einer Woche hätte man nicht mehr in der Wohnung bleiben können und der Täter 7 sei – ohne Frau und Kind – in ein Hotel gegangen. Er habe sodann wieder zurück nach Rumänien fahren wollen. Zudem hätte er bislang kein Geld erhalten und außerdem den Eindruck gehabt, dass Täter 7 sowie dessen Umfeld nicht die besten Absichten gehabt hätten. Allerdings habe der Täter 7 ihn zum Bleiben und zu einer neuen Tat überredet, bei der sodann die Festnahme erfolgt sei.
Den Aussagen des Täters 6 war zu entnehmen, dass es mindestens zwei Taten gab. Über die angeklagte Tat hinaus wurde nichts ermittelt.

Anmerkung
Ob das Gericht die persönlichen Angaben des Täters 6 als glaubhaft eingestuft hat, ist der Akte nicht zu entnehmen. Hinsichtlich der Darstellung des Tatablaufs war das Gericht von der Glaubhaftigkeit überzeugt. Mit Ausnahme der Erklärungen, wie sie sich kennengelernt haben.

Fall 7a, Täter 7	
Strafrechtliche Einordnung:	§§ 149, 152b, 303b, 22, 23, 25, 52 StGB
Tatzeit:	April 2007
Verfahrensausgang:	Freiheitsstrafe, 1 Jahr und 3 Monate; Strafaussetzung zur Bewährung
Finanzieller Schaden (Cashing):	0 €
Zum Täter:	Geboren 1968 Rumänischer Staatsangehöriger Männlich Verheiratet, ein Kind Bildungsabschluss nicht bekannt Berufsabschluss nicht bekannt

Sachverhalt

Aufgrund des Alarms eines Anti-Skimming-Moduls kontrollierten Polizeibeamte einen Geldautomaten, stellten die Manipulation mittels Skimming-Technik fest und kontrollierten im Nahbereich des Geldautomaten zwei verdächtige Personen (siehe Fall 6, Täter 6). Im Rahmen der körperlichen Durchsuchung der Täter 7 und 6 wurden Skimming-Utensilien aufgefunden. Gegen beide Täter wurde Untersuchungshaft angeordnet.

Zur Person

Täter 7, rumänischer Staatsangehöriger, war zum Tatzeitpunkt 39 Jahre alt und noch nicht polizeilich in Erscheinung getreten (kein Eintrag im Bundeszentralregister, keine polizeilichen Erkenntnisse).

Täter 7 war eigenen Angaben zu Folge zum Tatzeitpunkt verheiratet und hatte mit seiner Ehefrau ein gemeinsames Kind. In Rumänien habe er für monatlich umgerechnet etwa 150 € als Kellner gearbeitet. Diese Arbeitsstelle habe er über seine Ehefrau erhalten, die für umgerechnet etwa 150 € monatlich als Köchin beschäftigt ist.

Zur Tat/zu den Taten

Täter 7 sagte aus, er selbst sei der Ideengeber gewesen. Den Täter 6 habe er gebraucht, da die Technik so groß war und es daher besser gewesen sei, zu zweit an den Geldautomaten heranzugehen. Den Täter 6 habe er in einem Supermarkt in der Nähe seiner Unterkunft in Deutschland angesprochen. Die Skimming-Utensilien habe er von einem Albaner erhalten. Dieser hätte ihm für die Daten anschließend umgerechnet etwa 1.000 € geben wollen, wovon er die Hälfte dem Täter 6 habe geben wollen. Der Albaner hätte gebrochen Rumänisch gesprochen und gesagt, er habe öfter mit rumänischen Personen Kontakt. Das Gerät hätte er diesem zurückgeben sollen.

Den Aussagen des Täters 6 war zu entnehmen, dass es mindestens zwei Taten gab. Über die angeklagte Tat hinaus wurde nichts ermittelt.

Anmerkung

Ob das Gericht die persönlichen Angaben des Täters 7 als glaubhaft eingestuft hat, ist der Akte nicht zu entnehmen. Hinsichtlich der Darstellung des

Tatablaufs war das Gericht von der Glaubhaftigkeit überzeugt. Mit Ausnahme der Erklärungen, wie sie sich kennengelernt haben.

Fall 7b, Täter 7	
Strafrechtliche Einordnung:	§§ 202a, 152b, 263a StGB
Tatzeit:	Februar 2007
Verfahrensausgang:	Einstellung gemäß § 154 I StPO mit dem Hinweis auf ein weiteres Verfahren (Fall 7a)
Finanzieller Schaden (Cashing):	ca. 3.310 €
Zum Täter:	Geboren 1968 Rumänischer Staatsangehöriger Männlich Verheiratet, ein Kind Bildungsabschluss nicht bekannt Berufsabschluss nicht bekannt

Sachverhalt

Im Zuge der Festnahme des Täters 7 (siehe Fall 7a) wurde in der persönlichen Habe des Täters 7 eine Testkarte aufgefunden. Ein Abgleich dieser Testkarte mit vorherigen Tatorten führte zu einer weiteren Straftat. Die zu dieser Straftat vorliegenden Überwachungsbilder zeigten den Täter 7. Insofern konnte diese Straftat im Nachhinein geklärt werden.

Zur Person

siehe Fall 7a.

Zur Tat/zu den Taten

Die nachträgliche Aufklärung dieser Tat zeigt, dass es sich für den Täter 7 im Fall 7a nicht um die erste Tat handelte.

Anmerkung

Ohne.

Fall 8, Täter 8	
Strafrechtliche Einordnung:	§§ 152b, 149, 25 StGB

Tatzeit:	Juli 2007
Verfahrensausgang:	Freiheitsstrafe, 1 Jahr
Finanzieller Schaden (Cashing):	0 €
Zum Täter:	Geboren 1979 Männlich Rumänischer Staatsangehöriger Lebensgefährtin, ein Kind Ohne Schulabschluss Ohne Berufsabschluss In Rumänien vorbestraft (Eigentumsdelikte)

Sachverhalt

Aufgrund des Alarms eines Anti-Skimming-Moduls kontrollierten Polizeibeamte einen Geldautomaten und stellten die Manipulation mittels Skimming-Technik fest. Durch die Videoüberwachung der Tatörtlichkeit (öffentlicher Platz) lagen Bilder zweier Täter vor. Mithilfe dieser Bilder konnten die beiden Täter 8 und 9 (siehe Fall 9) in örtlicher und zeitlicher Nähe zum Tatort angetroffen und festgenommen werden. Gegen beide Täter wurde Untersuchungshaft angeordnet.

Zur Person

Täter 8, rumänischer Staatsangehöriger, war zum Tatzeitpunkt 27 Jahre alt. Nach Erkenntnissen des Bundeskriminalamtes war er in Rumänien wegen Autodiebstahls vorbestraft. Zum Zeitpunkt der Inhaftierung wurde er von den rumänischen Behörden zur Verbüßung einer weiteren dreijährigen Haftstrafe wegen Diebstahls und qualifizierten Diebstahls gesucht. Zudem wurden Skimming-Straftaten des Täters 8 in München und Stuttgart, unmittelbar vor der Festnahme in Frankfurt a.M., bekannt. Diese waren nicht Gegenstand des Verfahrens. Im Bundeszentralregister gab es keinen Eintrag.

Täter 8 hatte eigenen Angaben zu Folge keinen Schulabschluss. Nachdem Verlassen der Schule habe er als Handelsvertreter gearbeitet. Hierbei habe er umgerechnet etwa 150-200€ monatlich verdient. Er gab an, mit seiner Lebensgefährtin sowie einem gemeinsamen Kind zu leben. Da Täter 8 seine Arbeit etwa zwei Monate vor der Tat verloren habe, sei er nach Deutschland

gereist, um dort Geld zu verdienen. Mit dieser Reise habe er sich auch der Verbüßung einer Freiheitsstrafe entzogen.

Zur Tat/zu den Taten

In München habe Täter 8 den Täter 9 kennengelernt. Dieser habe ihm angeboten, ein Rückfahrtticket nach Rumänien zu bezahlen, wenn er mit ihm einen Geldautomaten manipuliere. Zusammen sei man nach Frankfurt gefahren und habe an einem Geldautomaten Zusatzelektronik montiert. Sofort sei man festgenommen worden.

Nähere Angaben zur Kontaktaufnahme mit dem Täter 9 (gleicher Geburts- und Wohnort), zur Erlangung des Skimming-Materials sowie zur geplanten Weitergabe der Daten und Entlohnung sind der Ermittlungsakte nicht zu entnehmen.

Anmerkung

Die Glaubhaftigkeit der persönlichen Angaben des Verurteilten wurde seitens des Gerichts nicht angezweifelt.

Fall 9, Täter 9	
Strafrechtliche Einordnung:	§§ 149, 152b, 25, 74 StGB, 1, 105 JG
Tatzeit:	Juli 2007
Verfahrensausgang:	Jugendstrafe, 2 Jahre und 6 Monate; Aufhebung des Urteils nach Berufung, sodann Jugendstrafe, 1 Jahr und 3 Monate
Finanzieller Schaden (Cashing):	0 €
Zum Täter:	Geboren 1988 Männlich Rumänischer Staatsangehöriger Ledig Realschule Besuch des Gymnasiums geplant

Sachverhalt

Aufgrund des Alarms eines Anti-Skimming-Moduls kontrollierten Polizeibeamte einen Geldautomaten und stellten die Manipulation mittels Skimming-Technik fest. Durch die Videoüberwachung der Tatörtlichkeit (öffentlicher

Platz) lagen Bilder zweier Täter vor. Mithilfe dieser Bilder konnten die beiden Täter 9 und 8 (siehe Fall 8) in örtlicher und zeitlicher Nähe zum Tatort angetroffen und festgenommen werden. Gegen beide Täter wurde Untersuchungshaft angeordnet.

Zur Person

Täter 9, rumänischer Staatsangehöriger, war zum Tatzeitpunkt 19 Jahre alt. Im Laufe der Ermittlungen konnten dem Täter 9 weitere Taten in Frankfurt, München, Wiesbaden und Mainz zugeordnet werden. Diese Taten waren nicht Gegenstand dieses Verfahrens. Ein Eintrag im Bundeszentralregister bestand nicht.

Täter 9 lebte eigenen Angaben zu Folge mit seiner Schwester bei seinen Eltern. Familiär gäbe es keine Probleme. Nachdem er den Realschulabschluss erlangt hatte, habe er ab Herbst den Besuch des Gymnasiums geplant. In der Schule hätte er mittelmäßige Leistungen erbracht. Später habe er die Marinehochschule besuchen wollen. Wegen gesundheitlicher Probleme sei er erst mit acht Jahren eingeschult worden.

Gegen das Urteil legte der Angeklagte Berufung ein. Die Berufung wurde verworfen, das angefochtene Urteil des Amtsgerichts im Rechtsfolgenausspruch aufgehoben. Die Kammer des Landgerichts monierte die Anwendung des Jugendgerichtsgesetzes. Sie stellte dar, dass der Angeklagte eine selbstbewusste Persönlichkeit zeigte, die sich vom Elternhaus abnabelte. Auch handele es sich bei den Taten nicht um Jugendverfehlungen. Für den Angeklagten sprächen jedoch sein junges Alter und die geständige Einlassung. Im Rahmen einer Gesamtabwägung wurde eine geringere Freiheitsstrafe als tat- und schuldangemessen erachtet.

Zur Tat/zu den Taten

In den Schulferien habe er Geld verdienen wollen, um sich ein Auto zu kaufen. Seinen Eltern, zu denen er einen guten Kontakt habe, habe er nicht gesagt, was genau er in Deutschland machen wolle. Er habe lediglich erzählt,

dass er sich einen Ferienjob suchen und bei Bekannten wohnen wolle. Stattdessen habe er Geldautomaten manipulieren wollen.
Nähere Angaben zur Kontaktaufnahme mit dem Täter 8(gleicher Geburts- und Wohnort), zur Erlangung des Skimming-Materials sowie zur geplanten Weitergabe der Daten und Entlohnung sind der Ermittlungsakte nicht zu entnehmen.

Anmerkung
Die Glaubhaftigkeit der persönlichen Angaben des Täters wurde seitens des Gerichts nicht angezweifelt.

3.1.3 Analyse der Daten

Alle neun Täter waren männlich. Zum Zeitpunkt der Tat waren sie zwischen 20 und 49 Jahre alt (drei Personen waren 20 Jahre alt, eine Person 21). Sieben Personen stammten aus Rumänien, zwei aus Bulgarien. Die beiden Personen aus Bulgarien waren Mittäter und stammten beide aus der gleichen Stadt (Bansko). Ebenso stammten zwei rumänisch stämmige Mittäter aus der gleichen Stadt in Rumänien (Bacău). Die anderen Täter stammten aus unterschiedlichen Städten. Vier Personen waren ledig, eine Person geschieden, fünf verheiratet bzw. in einer festen Lebenspartnerschaft mit einem Kind bzw. Kindern.

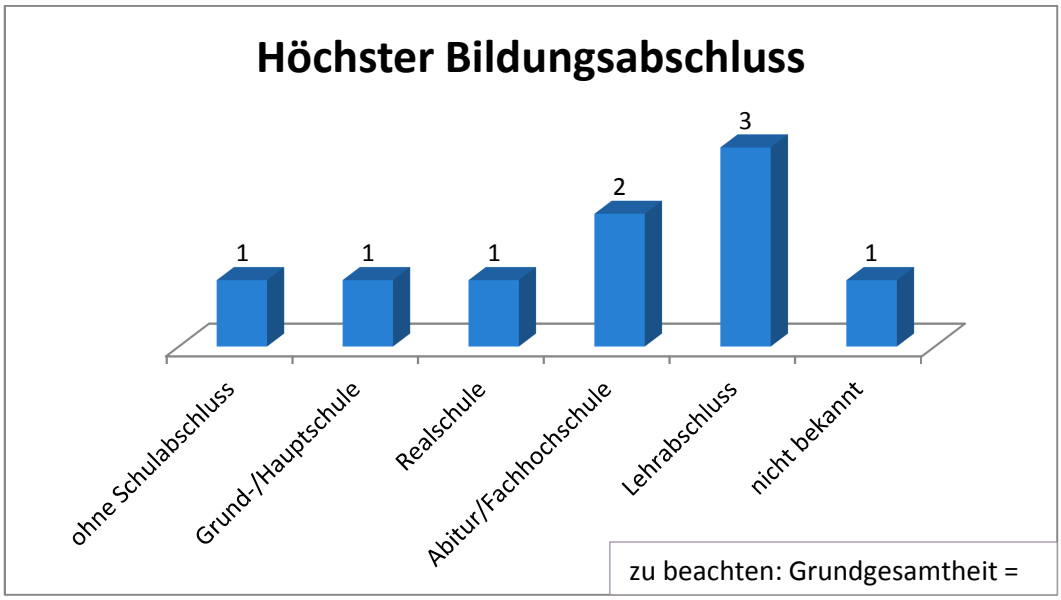


Abbildung 6: **Höchster Bildungsabschluss, Anzahl der Personen**
Eigene Statistik nach Auszählung

Eine der drei Täter mit Lehrabschluss hat Kraftfahrer gelernt und arbeitete nach eigenen Angaben sporadisch in diesem Berufsfeld. Ein weiterer hat Skilehrer und Monteur gelernt und arbeitete zur Zeit der Tat als Skilehrer. Sein Mittäter hat auch als Skilehrer und Skiliftarbeiter gearbeitet, eigentlich aber Schlosser gelernt. Einer der Täter mit Abitur hatte angegeben, ungelernte Arbeiten verrichtet zu haben. Eigentlich habe er in Spanien in der Baubranche gearbeitet, nach der Immobilienkrise jedoch keine feste Anstellung mehr gefunden. Der andere Täter mit Abitur studierte eigenen Angaben zu Folge Informatik und lebe von einer „Leistungs-Stipendiums-Zulage“ in Höhe von umgerechnet ca. 100€ monatlich und der Unterstützung seiner Tante. Die Person, deren höchster Bildungsabschluss nicht bekannt ist, gab an, eine Aushilfstätigkeit als Kellner ausgeübt zu haben. Der Täter ohne Schulabschluss habe als Handelsvertreter gearbeitet. Der Täter mit Grund-/Hauptschulabschluss gab an, zur Zeit der Tat arbeitslos gewesen zu sein. Mindestens sieben von neun Tätern haben einen Schulabschluss, dennoch gaben acht Personen an, arbeitslos gewesen zu sein bzw. nur saisonal/als Aushilfskraft Arbeit gehabt zu haben. Dabei hatte die Mehrheit der Täter Familie und Kinder zu versorgen, was aufgrund der schlechten Arbeitslage nicht oder nur unzureichend möglich sei. Zwei Täter gaben zudem an, hohe Schulden zu haben. Täter 4 habe sich beispielsweise Geld für eine Augenoperation des Großvaters geliehen. Dabei sei er von einem normalen Kredit ausgegangen. Letztlich sollte der Täter seine Schulden durch Skimming-Straftaten abarbeiten.

Zu einem Täter ging aus der Akte hervor, dass er in Rumänien wegen Eigentumsdelikten vorbestraft war. In den anderen Fällen wurde kein Rechtshilfeersuchen gestellt bzw. es ging keine Antwort ein. Keiner der Täter hatte einen Eintrag im Bundeszentralregister. Allerdings zeigten die polizeilichen Ermittlungen bei sechs Tätern weitere Skimming-Straftaten in anderen Städten vor der vorläufigen Festnahme in Frankfurt am Main auf. Einem dieser Täter konnten nicht nur weitere Skimming-Straftaten in anderen deutschen Städten zugeordnet werden, sondern dem BKA lagen weitere Informationen zu einer in Italien gegen Täter 2 verhängten Haftstrafe wegen Fälschung von Zahlungskarten vor. Auch aktuell war er wegen dieses Deliktes von Italien

zur Fahndung ausgeschrieben. Ein weiterer Täter war in Spanien wegen Skimming-Straftaten verurteilt worden. Insofern waren nur bei einem von neun Tätern (Täter 5) keine vorausgegangenen Skimming-Straftaten bekannt.
Inwieweit die Täter nach der untersuchten Tat erneut (einschlägig) straffällig geworden sind, war den Ermittlungsakten in sieben Fällen nicht zu entnehmen. Zwei Täter wurden erneut verurteilt. Täter 2 wurde etwa ein Jahr nach der untersuchten Tat vom Amtsgericht Darmstadt wegen gemeinschaftlichen Einbruchsdiebstahls zu einer Freiheitsstrafe von 8 Monaten verurteilt, zudem bestand ein Suchvermerk der Staatsanwaltschaft Hamburg (Strafverfolgung; das zu Grunde liegende Delikt war der Akte nicht zu entnehmen). Täter 9 wurde im Anschluss an das untersuchte Strafverfahren vom AG Frankfurt wegen einer erneuten Skimming-Straftat verurteilt. Hinzu kam ein Urteil des AG Passau wegen Verstoßes gegen § 9 FreizügG/EU[31] sowie ein Suchvermerk der Staatsanwaltschaft Wiesbaden (aus Gründen der Strafverfolgung; Delikt nicht erkennbar).

Sieben Täter gaben an, die Skimming-Utensilien von anderen Personen erhalten zu haben. Bei zwei Personen ging aus den Ermittlungsakten nicht hervor, wie sie an die Geräte gekommen sind. Bei acht Tätern erfolgte die Tatausführung nicht alleine. Lediglich Person 2 gab an, alleine gehandelt zu haben. Die Technik hätten sie aber an einen „Ansprechpartner“ weitergeben und dafür Geld erhalten wollen. Auch wenn das Manipulieren der Geldautomaten alleine durchgeführt wurde, wären für die weiteren Schritte Mittäter/Hintermänner von Nöten gewesen.

In vier Fällen konnten die Ermittlungsbehörden durch die vorläufige Festnahme das Cashing und somit finanzielle Schäden verhindern. In drei Fällen wurde mit den Kartendaten von 40 betroffenen Bankkunden Bargeld in Höhe von knapp 45.000 € abgehoben. Die Einsätze der gefälschten Zahlungskarten (Kartendubletten) erfolgten dabei in den Niederlanden und den USA.

[31] Einreise bzw. Aufenthalt im Bundesgebiet der BRD trotz Verlust des Rechtes hierauf.

Im Rahmen der digitalforensischen Auswertung[32] der sichergestellten Skimming-Utensilien stellten Polizeibeamte die Hochwertigkeit der Technik im zweiten Fall (bei Täter 2) fest. Die Variante dieser Technik war den Ermittlern zuvor nicht bekannt gewesen. Es wurden Originalbauteile eines Geldautomaten verwandt, so sei die Manipulation kaum zu erkennen gewesen.

Hinsichtlich der Auswahl des Tatorts gaben fünf Täter an, nach einem „passenden“ Geldautomaten-Modell gesucht zu haben, an das die Skimming-Technik montiert werden konnte. Die anderen vier Täter sagten aus, die Tatorte seien ihnen durch andere Personen/Hintermänner vorgegeben worden. Nach Auswertung der Ermittlungsakten ist davon auszugehen, dass es sich bei allen neun Tätern um sogenannte Läufer handelte. Auch wenn Täter 2 angab, „selbstständig“ gehandelt zu haben, war er hinsichtlich des Cashings von einer weiteren Person abhängig gewesen.
Neben der Methode, die Skimming-Geräte mit abgegriffenen Kartendaten an einen „Ansprechpartner“ weiterzugeben (Täter 2), sollten die abgegriffenen Daten in zwei Fällen über das Internet an Hintermänner übermittelt werden. Den Läufern wurde zu diesem Zweck ein Laptop zur Verfügung gestellt. In den anderen Fällen ist die Übertragung der Daten nicht bekannt.

Hinsichtlich der Bezahlung der Läufer wurden verschiedene Möglichkeiten angesprochen. Täter 1 gab an, 250 bis 300€ pro manipulierten Geldautomaten erhalten zu haben, Täter 5 seien 500 bis 1.000 € versprochen worden. Täter 2 gab an, ihm seien 10 bis 15% vom Gesamterlös versprochen worden, was einige Tausend Euro bedeutet hätte. Den Tätern 4 und 5 seien 50 $ pro abgegriffenem Kartensatz versprochen worden. In den anderen Fällen sei kein fester Betrag vereinbart worden bzw. die Art und Höhe der Bezahlung ist den Ermittlungsakten nicht zu entnehmen.

Acht Täter wurden rechtskräftig verurteilt. Bei einem Täter wurde das Verfahren unter Hinweis auf ein anderes Skimming-Verfahren gemäß § 154 Abs. 1 StPO eingestellt. Täter 1 wurde zu einer Freiheitsstrafe von 4 Jahren verurteilt. Dies stellt die höchste, verhängte Freiheitsstrafe dar.

[32] Auswertung von Speichereinheiten, Kameraeinheiten, etc.

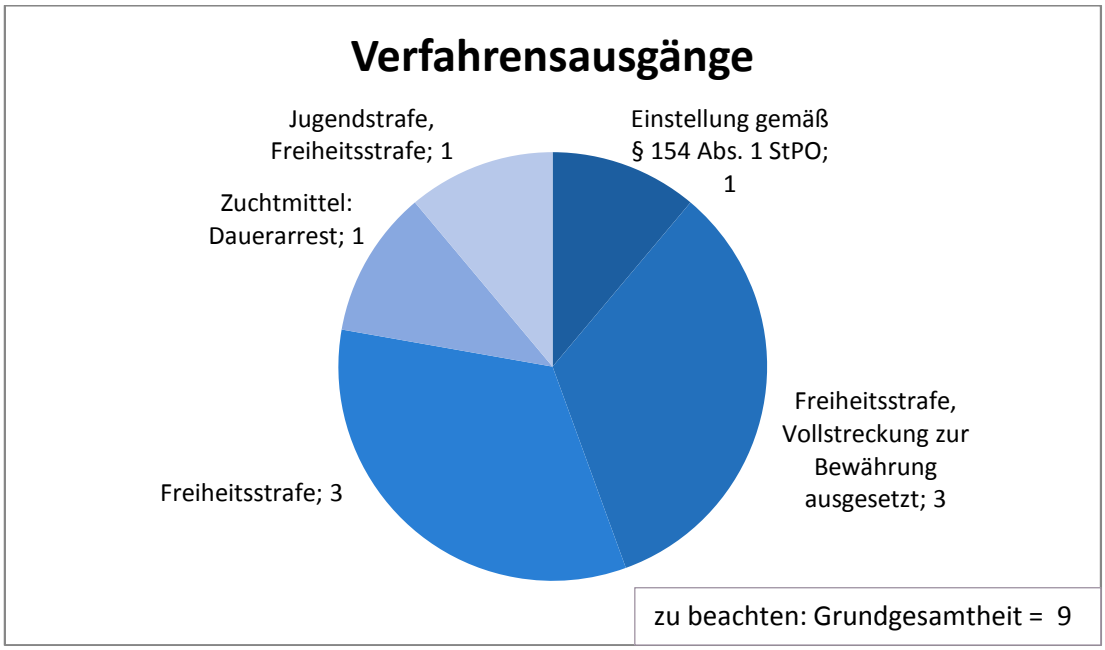


Abbildung 7: **Verfahrensausgänge in Jahren**
Eigene Statistik nach Auszählung

3.2 Schriftliche Befragung von Experten

In Ergänzung der Inhaltsanalyse wurde, als weitere explorative Methode, eine schriftliche Befragung von Polizeibeamten der rumänischen und bulgarischen Strafverfolgungsbehörden sowie von einem Sachverständigen für „Cybersicherheit“ an der University of Library Studies and Information Technologies (ULSIT) in Sofia, durchgeführt. Das Arbeitsfeld aller befragten Personen umfasst die Bearbeitung bzw. die Begutachtung von Skimming-Straftaten.

3.2.1 Feldzugang, Erhebung der Daten und Methodik

Ausgewählt wurden Personen aus den Länder Rumänien, Bulgarien und den USA, die Beamten des Polizeipräsidiums Frankfurt am Main durch gemeinsame Ermittlungsverfahren oder internationale Fortbildungsveranstaltungen persönlich oder zumindest namentlich bekannt waren. Insgesamt fanden sich zehn Kontaktadressen von Personen, die in ihrer täglichen Arbeit mit dem Phänomen Skimming befasst waren. Nach Bogner und Menz verfügt ein Experte über „*technisches, Prozess- und Deutungswissen, das sich auf sein spezifisches professionelles oder berufliches Handlungsfeld bezieht. Insofern besteht das Expertenwissen nicht allein aus systematisiertem, reflexiv zugänglichem Fach- oder Sonderwissen, sondern es weist zu großen Teilen den Charakter von Praxis oder Handlungswissen auf*“ (Das Experteninter-

view 2002, S. 46). Der Expertenbegriff wird demnach weiter gefasst. Die fehlende Sachverständigeneigenschaft ist kein Ausschlusskriterium. Bei der Auswertung ist zu beachten, dass die Aussagen der hier gewählten Personen von jeweils individuellen, sozialen Deutungsmustern und Orientierungen abhängen können (Das Experteninterview 2002, S. 46), da der Experte auch Privatmensch ist (Flick 2009, S. 216).

Um das Expertenwissen abzurufen, wurde ein einheitlicher schriftlicher Fragebogen („questionnaire“) erstellt, in die englische Sprache übersetzt und sodann an die zehn Personen versandt. In einem Anschreiben wurde den Personen der Hintergrund der Befragung dargelegt, um die Rücklaufquote zu erhöhen. Den Personen wurde angeboten, in der jeweiligen Muttersprache antworten zu können. Etwaige sprachliche Missverständnisse oder Hemmnisse sollten hierdurch vermieden werden.

Bei der Zusammenstellung des Fragebogens wurde insbesondere Wert auf die Einleitungsfragen gelegt. Zu Beginn wird die befragte Person gebeten, ihre berufliche Tätigkeit – und damit einhergehend die Erfahrung im Umgang mit Skimming-Delikten – darzustellen. Hierdurch soll dem Befragten aufgezeigt werden, über welches Wissen er verfügt und weshalb eine Befragung seiner Person bedeutsam ist. Für die Auswertung der Antworten sind diese Informationen wichtig, um die Angaben einordnen zu können. Anschließend folgen Fragen zur eigentlichen Thematik, trichterförmig angeordnet: anfangs allgemeine Fragestellungen, bis hin zu konkreten Fragen. Zu den einzelnen Themenbereichen wurden zumeist mehrere Fragen gestellt, auch im Hinblick auf eine fehlende Interviewsituation und mögliche Missverständnisse. Bei den Fragen handelt es sich überwiegend um offene Fragen. Einleitend wurden die Befragten gebeten, möglichst umfangreich zu antworten und Aussagen zu erklären. Zudem wurde darauf hingewiesen, dass die Erfassung über den Fragebogen hinausgehender Aspekte, die dem Befragten von Bedeutung erscheinen, erwünscht ist.

Vier Personen sandten einen ausgefüllten Fragebogen zurück, zwei Personen aus Bulgarien und zwei Personen aus Rumänien. Die Antworten können in den Anlagen nachgelesen werden (siehe S. 105, 108, 113, 116). Drei Personen antworteten auf Englisch, eine Person auf Bulgarisch. Dieser Frage-

bogen wurde von einem staatlich geprüften und ermächtigten Übersetzer in die deutsche Sprache übertragen.
Die Auswertung der Daten erfolgte manuell und nach Themenfeldern sortiert. Besonders markante Aussagen wurden zitiert. Etwaige Rechtschreibfehler wurden dabei ohne Kommentar übernommen. Insbesondere in den englischen Texten finden sich Fehler. Diese mindern das Verständnis der Aussagen jedoch nicht. Zum besseren Verständnis findet sich in der Fußnote eines jeden englischen Zitats eine Übersetzung in die deutsche Sprache. Diese wurde von der Verfasserin angefertigt. Sie entsprechen keiner professionellen Übersetzung, geben jedoch den Sinn der Aussage voll umfänglich wieder. Entsprechend dem Rücklauf der Fragebögen wurden diese mit „Experte 1“ bis „Experte 4“ gekennzeichnet, um das Zitieren einzelner Textpassagen trotz Anonymisierung zu ermöglichen.

3.2.2 Analyse der Daten

Kennzeichnend für alle Befragten ist deren langjährige Erfahrung im Arbeitsbereich „Skimming“. Die Experten gaben an, zwischen sieben und vierzehn Jahren Erfahrung mit der Bearbeitung von Skimming-Delikten zu haben. Drei der Experten haben als Sachbearbeiter gearbeitet bzw. leiten zwischenzeitlich eine Abteilung. Experte 2 gab an, als technischer Sachverständige zu arbeiten. Durch die Auswertung von Skimming-Bauteilen konnte dieser spezielles Wissen im Bereich Technik sammeln. Zwei der Experten stammten aus Bulgarien, zwei aus Rumänien. Inhaltlich sind keine Unterschiede zwischen beiden Ländern erkennbar.

Auf die Frage hin, wie eine Skimming-Bande organisiert ist, gaben alle Befragten an, eine strenge Hierarchie erfahren zu haben: „*Suspects are very well organized in OCGs*[33]*, having specific roles and* ***hierarchies****, in order to obtain illegal profits*“[34] (Experte 1, Antwort zu Frage 2, Seite 105). In den meisten Fällen gebe es einen Anführer, weitere Verantwortliche für die verschiedenen Teilbereiche (Bau/Anschaffung von Skimming-Geräten, Logistik/Unterkunftsplanung, Manipulation der Geldautomaten, Transfer der „ab-

[33] Englisch Organized crime gangs/groups – Gruppe der Organisierten Kriminalität
[34] *Die Tatverdächtigen sind in hierarchisch strukturierten Gruppen/Banden organisiert, wobei spezifische Rollen vergeben sind, um den Profit zu maximieren.*

gegriffenen Bankdaten, Aufbereitung der Bankdaten, Fälschung von Zahlungskarten, Cashing, Transfer des Geldes) und Ausführende. In diesem Zusammenhang ist eine Äußerung interessant: „*The activities oft he groups are divided in such a way that one or two groups may not be able to close the circle of all the activities and carry out the crime from end to end*"[35] (Experte 2, Antwort zu Frage 3, Seite 108). Experte 4 führte aus, dass „*sich die unterschiedlichen Organisationsstufen untereinander nicht kennen*" (Experte 4, Antwort zu Frage 2, Seite 116). Die klare Aufgabenverteilung und die hierarchische Organisation stärkten die Position des Bandenchefs. Experte 3 führte zu dieser Thematik aus: „*One´s opinion counts more in these groups usually being the person who has more money and who invest in buying the skimming equipment*"[36] (Experte 3, Antwort zu Frage 4, Seite 113). Für die Begehung von Skimming-Straftaten seien ein "Grundkapital" sowie ein Netzwerk von Nöten.

Dies führt zu einem weiteren interessanten Aspekt. Die Experten 1, 2 und 4 sprachen von sogenannten „*Maultieren"/"Mauleseln*" (Experte 1, Antwort zu Frage 3, Seite 105, Experte 2, Antwort zu Frage 12, Seite 108 und Experte 4, Antwort zu Frage 3, Seite 116). Hierbei handelt es sich um Bandenmitglieder niederen Ranges, welche für den Transport von Skimming-Equipment, die Manipulation der Geldautomaten oder zu Zwecken der Geldwäsche benötigt werden. Experte 3 führte aus, dass die risikoreichen Manipulationen von Geldautomaten durch „*newcommers or very poor people who are willing to assume the risks*"[37] (Experte 3, Antwort zu Frage 13, Seite 113) erledigt werden. Einzig Experte 2 differenzierte hinsichtlich der Personen, die Skimming-Geräte anbringen. Er habe Fälle kennengelernt, in welchen das Skimming-Equipment von Amateuren angebracht worden sei, die in einer Bar rekrutiert worden seien. Die Auswertung von Überwachungsbildern aus Bankinstituten habe ihm aber gezeigt, dass in den meisten Fällen professionelle Täter agierten. Zu diesem Schluss komme er, da diese Täter das Skimming-Equipment

[35] *Die Aktivitäten einer Bande sind in separate Teile gegliedert, sodass es ein oder zwei Untergruppen nicht möglich ist, die gesamte Kette an Aktivitäten durchzuführen und sich „selbstständig" zu machen.*
[36] *Für gewöhnlich zählt die Meinung desjenigen in einer Gruppe am meisten, der das meiste Geld hat und in den Kauf von Skimming-Equipment investieren kann.*
[37] *Neulinge oder sehr arme Personen, die das Risiko auf sich nehmen.*

in wenigen Sekunden angebracht hätten und dabei so vorgehen (Anmerkung: vermutlich Vermummung durch Kleidungsstücke), dass man diese anhand der Bilder nicht wieder erkennen könne. Es kann kritisch hinterfragt werden, ob das Anbringen der Skimming-Technik in kurzer Zeit sowie das Achten auf Verdeckung des Gesichts für die Beschreibung „professionell" ausreichend ist. Entscheidend ist die Übereinstimmung aller vier Experten über das Anwerben von „Neulingen" oder Personen mit Schulden, um die risikoreichen Arbeiten an diese delegieren zu können. Durch den Begriff des „Maultieres" wird dies bildhaft.

„*In den meisten Fällen werden nur die Personen festgenommen die Skimmer montieren, es ist schwierig bis zu den Organisatoren zu gelangen*" (Experte 4, Antwort zu Frage 13, Seite 116). Die Bandenchefs stammen nach Aussagen der Befragten aus Rumänien und Bulgarien. Dort halten sie sich vorwiegend auf, außer um spezielle Dinge zu regeln oder: „*he may want to supervise closely the group activities to maximise profit*"[38] (Experte 3, Antwort zu Frage 5, Seite 113). „*The real organizers of skimming criminal activity remain hidden for police sources*"[39] (Experte 2, Antwort zu Frage 5, Seite 108). Die Kommunikation innerhalb der Gruppierung sowie die Kontrolle durch den Bandenchef erfolge über Mobiltelefon, Internet, Skype oder Viber[40]. „*The bosses in the structure decide what group, where should work and instruct the leader of the group left. Even abroad, leaders of groups periodically make status reports of their seniors, using Skype or phone*"[41] (Experte 2, Antwort zu Frage 14, Seite 108).

Ein Betrachtungsschwerpunkt lag auf dem Bereich der Skimming-Technik. Insbesondere Experte 2 konnte hierzu umfangreich antworten. Nach dessen Angaben wird das Skimming-Equipment in sogenannten „*factories*"[42] (Experte 2, Antwort zu Frage 7, Seite 108) hergestellt. Hierbei kann es sich zum

[38] *Er möchte die Aktivitäten der Gruppe streng überwachen, um den Profit zu maximieren.*
[39] *Die eigentlichen Organisatoren von Skimming-Aktivitäten bleiben den Polizeibehörden verborgen.*
[40] Eine Voice over IP-Software (=VoiP) für Computer und Smartphones, die kostenloses Telefonieren über das Internet ermöglicht.
[41] *Die Chefs der Hierarchie entscheiden, welche Gruppe an welchem Ort arbeiten soll und instruieren den Leiter der Gruppe. Selbst im Ausland geben die Gruppenleiter über Skype oder Telefon regelmäßige Statusberichte an ihre Chefs ab.*
[42] Englisch factory – Werkstätten/Fabriken

einen um eine Wohnung handeln, aber auch um eine Fabrik, in der Elektronikartikel gefertigt werden. Grundsätzlich seien drei Typen von Skimming-Equipment zu unterscheiden: Gewöhnliches Skimming-Equipment greife auf Bauteile von MP3- oder MP4-Playern[43] zurück und könne in einer Wohnung oder einer Garage gefertigt werden. Spezielle Skimming-Geräte seien von Spezialisten gebaut. Diese nutzten Elektronikfabriken zur Herstellung der Leiterplatten/Platinen – den wahren Zweck verschleiernd (vgl. ebenda). Zudem könne man Skimming-Equipment im Internet beziehen. Es gäbe verschiedene chinesische Firmen, die Magnetstreifenleser verkaufen[44].

Grundsätzlich setze die Herstellung von Skimming-Equipment technische Kenntnisse voraus. Experte 2 gab an, die meisten ihm bekannten „Techniker" aus Skimming-Gruppierungen seien Elektroingenieure oder Elektroniker mit großen Erfahrungswerten in der Produktion von Elektronikbauteilen. Häufig arbeite ein Team von Spezialisten aus den Bereichen Elektronik, Software, Computer und Kommunikation zusammen.

Die Herstellung erfolge überwiegend durch wenige Gruppen. Unter Angabe entsprechender Parameter könne Technik bestellt werden, sofern eine Gruppe nicht über einen „Techniker"/eine „Werkstatt" verfüge. Die einsatzbereite Technik käme in Warensendungen, getarnt in Spielzeugen oder Elektronikartikeln für den Heimbedarf, nach Deutschland. Ebenfalls brächten „Maultiere" dieses über die Grenze.

Die Angaben der Experten 1, 3 und 4 stützten die Ausführungen des Experten 2 hinsichtlich der Skimming-Technik.

Die an deutschen Geldautomaten abgegriffenen Daten gelangten nach Angaben der befragten Experten auf elektronischem Wege über das Internet (E-Mail, Instant Messaging[45]) oder auf Speichergeräten (USB-Sticks, Festplatten) zu den Bandenmitgliedern, die für die Aufbereitung der Daten zuständig sind. Teilweise würden diese Daten auch verkauft. Hierfür seien spe-

[43] Zumeist tragbare Geräte zur Wiedergabe von Audio- bzw. Videodateien

[44] Experte 2 verweist auf die Homepage: http://www.cardreaderfactory.com/magnetic-stripe-readers.html, zuletzt geprüft am 20.02.2014. Auf dieser Homepage sind Magnetstreifenleser in verschiedenen Ausführungen ab $699 verfügbar. Die Homepage http://www.alibaba.com/showroom/skimming-card-reader.html, zuletzt geprüft am 20.02.2014, bietet ebenfalls Magnetstreifenlesegerät in unterschiedlichen Ausführungen an.

[45] Nachrichtensofortversand über ein Computerprogramm; beispielsweise: Skype, Windows Live Messenger, Gajim.

zielle Homepages eingerichtet worden. Letztlich gelangten die Daten zum Cashing in andere Länder. Teilweise würden die Daten in verschiedenen Ländern gleichzeitig eingesetzt.

Das beim Cashing erhaltene Bargeld könne auf verschiedenen Wegen zur Bandenführung gelangen. Zum einen würden Personen mit den nach Zollvorschriften maximal erlaubten Bargeldsummen reisen. Zum anderen würde das Geld transferiert: Entweder über Bankkonten der sogenannten „Maultiere“ (Geldwäsche) oder aber über Bargeldtransferanbieter (z.B. Western Union, MoneyGram[46]). Beim Bargeldtransfer über diverse Anbieter würden Angehörige der Bandenmitglieder namentlich angegeben. Außerdem würden einige Bandenchefs den Kauf teurer Waren bevorzugen, wie etwa Luxuswagen. Diese würden dann in das Heimatland gebracht und dort verkauft werden.

Zur Bezahlung der einzelnen Bandenmitglieder würde ein Teil des erhaltenen Geldes innerhalb der Gruppierung verteilt, zumeist in bar. Ebenso würde es mit Verbindlichkeiten/Schulden verrechnet. Die Höhe der Bezahlung richte sich nach den Aufgaben des jeweiligen Mitgliedes und nach vorher vereinbarten Prozentsätzen.

Zu der Frage, ob sich Skimming-Straftäter von anderen Straftätern unterscheiden, gab Experte 2 an: „*Yes. The gangs that dealing with crimes against payment cards have a better organization and more strictly conrolled.*“ [47] (Experte 2, Antwort zu Frage 20, Seite 108). Experte 1 beschrieb Skimming-Täter wie folgt: „*Skimming offenders are creative, willing to take up risks, determined, proactive, dynamic, internationally minded*“[48] (Experte 1, Antwort zu Frage 20, Seite 105). Experte 3 weist auf zwei Aspekte hin: „*a Skimming offender is mostly non-violent, chasing to obtain easy money with minimum of risk. a Skimming offender is often tehnical well-*

[46] Die Firma MoneyGram International ermöglicht – ähnlich der Western Union AG – weltweiten Bargeldtransfer.

[47] *Ja. Die Gruppierungen, die Zahlungskartenkriminalität begehen, sind besser organisiert und strenger kontrolliert.*

[48] *Skimming-Täter sind kreativ, risikobereit, entschlossen, ergreifen die Initiative, dynamisch und international aufgeschlossen.*

prepared, having knowledge of the latest tehnologies related to skimming devices"[49] (Experte 3, Antwort zu Frage 20, Seite 113).
Die Experten 1 und 4 wiesen darauf hin, dass Skimming-Straftäter teilweise auch durch andere Straftaten in Erscheinung getreten sind: Diebstahl, Einbruch, Gewalttaten, (Schutzgeld-)Erpressungen, Drogenhandel, Menschenhandel, Prostitution.

Die Experten 1, 3 und 4 geben an, dass es örtliche Schwerpunkte gebe. So stammten viele bulgarische Skimming-Straftäter aus den Städten Sofia, Plovdiv und Silistra. Hier würden auch die „Maultiere" rekrutiert. Experte 2 führt aus, dass sich – eigenen statistischen Zahlen zufolge – der Großteil der „factories" in den größeren Städten Bulgariens befände. Ebenso sei dort die Bandenaktivität höher. In Rumänien seien vorwiegend die Städte Bacau, Craiova, Bukarest, Ramnicu Valcea für „*cybercrime offenders*"[50] (Experte 3, Antwort zu Frage 21, Seite 113) bekannt.
Nach Experte 1 ist ein Trend ersichtlich, wonach Skimming-Straftäter aus einer bestimmten Region in andere (größere) Städte umziehen oder mit Personen von dort in Kontakt treten.

Experte 3 äußerte darüber hinaus: „*The criminal groups from Romania often targeted countries like Italy, Spain, France where judicial authorities offered a weak response to Romania s judicial authorities or are known for easy punishments related to cybercrime phenomenon*[51]" (Experte 3, Antwort zu Frage 21, Seite 113).

Die nahezu ausschließliche Begehung von Skimming-Straftaten durch rumänische oder bulgarische Staatsangehörige erklären sich die Experten wie folgt:

[49] *Ein Skimming-Täter ist meist nicht gewalttätig. Er zielt darauf ab, leichtes Geld mit möglichst wenig Risiko zu machen. Ein Skimming-Täter ist meist technisch versiert, kennt sich mit den aktuellsten Technologien aus, die für Skimming-Equipment von Bedeutung sind.*
[50] *Straftäter, die Internetkriminalität begehen.*
[51] *Die Banden aus Rumänien begehen ihre Straftaten oft in Ländern wie Italien, Spanien oder Frankreich, da die dortigen Justizbehörden kaum mit rumänischen Justizbehörden zusammen arbeiten und Internetkriminalität wird in diesen Ländern weniger drastisch bestraft.*

„*There are multiple causes: economic context, EU developed payment marketplace, legislation*" (Experte 1, Antwort zu Frage 6, Seite 105) – so stellt Experte 1 ein Zusammenspiel verschiedener Faktoren dar.

Experte 2 fokussiert einen Ausbildungsschwerpunkt in den Branchen Elektronik und Computer: "*In the 80s of the 20th century, in Bulgaria and Romania education in computer science and Electronics was very good, also had many productions of various electronic devices.*

In the 90s, most of these industries were closed or went bankrupt, and many experts were left without work.

Some of these professionals immigrated to other countries, others changed their profession, but there are number of specialist who works for the criminals as they getting good money"[52] (Experte 2, Antwort zu Frage 6, Seite 108).

Auch Experte 4 erklärt sich diese Auffälligkeit durch die Anforderungen an Skimming-Täter. Es seien "*spezifische Kenntnisse und Fertigkeiten erforderlich, solche von IT-Spezialisten, Taschendieben für die Montage und Demontage der Skimmer an den Bankautomaten, sowie auch technisch versierte Personen*" (Experte 4, Antwort zu Frage 6, Seite 116).

Experte 3 führt aus, „*For example, if a group of people started this kind of activities at a certain time and they remained unpunished for a long time despite the fact that theirs wealth continuesly increased over the years, determined many young people to think that this kind of activities would increase their income and that this is a way to become wealthy*"[53] (Experte 3, Antwort zu Frage 21, Seite 113).

[52] *In den 80er Jahren des 20. Jahrhunderts war in den Ländern Bulgarien und Rumänien die Ausbildung in den Bereichen Informatik und Elektronik sehr gut, da dort viele elektronische Waren produziert wurden. In den 90er Jahren wurden die meisten dieser Fabriken geschlossen oder gingen insolvent, sodass viele Leute arbeitslos wurden. Einige der arbeitslosen Experten emigrierten in andere Länder, andere wiederum schulten um. Aber es blieb immer noch eine gewisse Anzahl an Experten übrig, die für eine gute Bezahlung Kriminellen zuarbeitet.*

[53] *Zum Beispiel: Wenn eine Gruppe mit dieser Art von Aktivität beginnt und für eine längere Zeit ungestraft davon kommt und zudem deren Wohlstand zunimmt, dann denken viele junge Leute, dass diese Aktivitäten ihr Einkommen erhöhen könnten und es ein einfacher Weg sei, um Geld zu verdienen.*

3.3 Interview eines rechtskräftig verurteilten Straftäters

Unter dem Aspekt der Triangulation wurde der Untersuchungsgegenstand – neben der Perspektive der Strafverfolgung – auch aus dem Blickwinkel eines Täters betrachtet. Eine Rolle, die Außenstehende schwerlich antizipieren können, weshalb die Ergebnisse möglicherweise eingeengte Denkmuster aufbrechen können.

3.3.1 Feldzugang, Erhebung der Daten und Methodik

Um persönliche Interviews mit rechtskräftig verurteilten Skimming-Straftätern durchführen zu können, wurde zuerst das Hessisches Ministerium der Justiz, für Integration und Europa um Genehmigung des Forschungsvorhabens im Justizvollzug gebeten. Diese Anfrage wurde negativ beschieden, da in den hessischen Vollzugsanstalten kein geeigneter Gefangener einsaß. Insofern wurde eine weitere Anfrage an den Kriminologischen Dienst des bayerischen Justizvollzugs gestellt. Die Anfrage wurde genehmigt. Insgesamt befanden sich in den Justizvollzugsanstalten Bayerns drei rechtskräftig verurteilte Straftäter. Über die jeweilige Anstaltsleitung wurde diesen Personen ein Anschreiben in ihrer Muttersprache zugeleitet (siehe S. 87). In dem Anschreiben wurde den Personen in kurzen Zügen der Inhalt der Arbeit – nicht das konkrete Thema der Befragung – sowie die Bedeutsamkeit einer Befragung dargestellt (vgl. Diekmann 2007, S. 486). Ebenso wurde die Anonymisierung der Ergebnisse zugesichert. Zwei Personen lehnten ein solches Interview ab. Letztlich erklärte sich ein Insasse zu einem Interviewtermin bereit. Aus rechtlichen Aspekten und um etwaige Missverständnisse zu vermeiden, wurden Personen in Untersuchungshaft nicht in die Anfrage einbezogen. Der skizzierte Ablauf stellt die mangelnde Verfügbarkeit geeigneter Interviewpartner dar. Eine Anfrage an die Justizbehörden weiterer Länder war aus zeitlichen Gründen nicht umsetzbar.

In Ergänzung zu den beiden bereits dargestellten Methoden sollte das Interview der weiteren Rekonstruktion des Bildes über Skimming-Täter sowie deren Beweggründen dienen. Insofern wurde die Erhebungsmethode des leitfadengestützten Interviews gewählt. Bei der Erstellung eines Leitfadens wurde das „*Prinzip der Offenheit*“ (Gläser und Laudel 2010, S. 115) dahin gehend berücksichtigt, dass ein breites Spektrum an Fragestellungen vorgege-

ben wurde. Damit sollte dem Befragten ermöglicht werden, sein Wissen und seine Erfahrungen wiedergeben zu können. Fragen nach Fakten wurden offen gestellt, um als Erzählanregung zu dienen. Um nach wichtigen Aspekten fragen zu können, die seitens der interviewten Person nicht genannt werden, dienten Nachfragen bzw. Detailfragen als Erinnerungshilfe (vgl. Gläser und Laudel 2010, S. 145). Zudem wurde dem Anspruch einer Operationalisierung Rechnung getragen, also „*die Aufgliederung und Übersetzung des wissenschaftlichen Erkenntnisinteresses in den Kommunikationsraum des Interviewpartners*“ (Gläser und Laudel 2010, S. 115). Es wurde somit Wert auf klare, verständliche Fragen gelegt. Ein Pre-Test und ggf. eine Anpassung des Fragebogens konnte nicht durchgeführt werden. Sowohl der explorative Charakter der Vorgehensweise, wie auch mangelnde Verfügbarkeit von Interviewpartnern ließen dies nicht zu.

Das Interview wurde als face-to-face Interview in den Räumlichkeiten der Justizvollzugsanstalt durchgeführt. Der Zeitpunkt des Interviews wurde durch den Befragten vorgegeben. Er bat um einen Termin zu einer gewissen Uhrzeit, da er in der Justizvollzugsanstalt einer regelmäßigen Tätigkeit nachgeht und diese für das Interview nicht absagen wollte. Da die befragte Person rumänischer Staatsangehöriger und somit der deutschen Sprache nur in Teilen mächtig war, war das Hinzuziehen eines Dolmetschers unverzichtbar. Durch die Übersetzung besteht die Gefahr des Informationsverlustes: Wortwahl, Satzstellung, Betonung, Prosodie können durch den Einsatz eines Dolmetscher verfälscht werden bzw. sind hierdurch nicht wahrnehmbar. Hinsichtlich der Sprachkenntnisse des Befragten gab es keine Alternative. Die Dolmetscherin wurde vor dem Interview gebeten, die Darstellungen des Befragten möglichst exakt in Wortwahl und Stimmlage wieder zu geben. Im Verlauf des Interviews zeigte sich, dass der Befragte die deutsche Sprache weitgehend verstehen kann. Sofern er fürchtete, seine Aussage wurde nicht richtig wieder gegeben, unterbrach er die Dolmetscherin bzw. ergänzte seine Aussage. Aufgrund dessen können die übersetzten Aussagen als authentisch eingestuft werden.
Während der Befragung war neben der Dolmetscherin auch ein Diplom-Psychologe der Justizvollzugsanstalt anwesend. Diesem war der Befragte

aufgrund der täglichen Arbeit in der Justizvollzugsanstalt bekannt. Auch hatte der Diplom-Psychologe dem Befragten das Anschreiben zugeleitet und mit ihm die freiwillige Teilnahme an dem Interview erörtert. Der Umgang des Diplom-Psychologen mit der befragten Person schien vertraut, sodass die Anwesenheit dessen nicht als Hemmnis eingeschätzt wurde. Dieser Eindruck bestätigte sich im Verlauf des Interviews.
Vor Beginn des eigentlichen Interviews stand die persönliche Kontaktaufnahme mit dem Insassen. Der Insasse schien auf die folgende Befragung gespannt zu sein und war darauf bedacht, im Hinblick auf die wissenschaftliche Arbeit sachdienliche Angaben machen zu können. Von Beginn an konnte eine Vertrauensbasis geschaffen werden. Die Gesprächsatmosphäre kann durchgehend als offen beschrieben werden. Die Ausgeglichenheit zwischen „Professionalität und Natürlichkeit“ (Gläser und Laudel 2010, S. 172) stand dabei im Vordergrund.
Im Vorgespräch zur Befragung wurde nochmals die Freiwilligkeit sowie eine Anonymisierung der Interviewinhalte angesprochen. Auch wurde dem Befragten erklärt, dass die Ergebnisse eines Interviews ausschließlich wissenschaftlichen Zwecken dienen und keinerlei negativen Konsequenzen hierdurch zu befürchten sind. Der Insasse gab an, zu einem Interview bereit zu sein und die Fragen im Rahmen seiner Möglichkeiten beantworten zu wollen.

Um das Interview in voller Gänze aufzuzeichnen, wurde eine Tonaufnahme vorgenommen. Die befragte Person hatte hiergegen keine Einwände (siehe S. 92). Die Audiodatei wurde mit Hilfe der Transkriptionssoftware „f4“ verschriftet. Die zugrunde gelegten Transkriptionsregeln sowie die Verschriftung des Interviews finden sich im Anhang (siehe S. 94 und S. 95).

Das Interview umfasste etwa 18 Minuten. Der Interview-Leitfaden trat in den Hintergrund, da die befragte Person angab, zwar aufgrund eines Skimming-Delikts festgenommen worden zu sein. Ursächlich für die mehrjährige Haftstrafe seien jedoch andere Straftaten (Eigentums- und Vermögensdelikte). Aufgrund der kurzen Interviewzeit, war der Umfang des Transkriptes übersichtlich. Zudem wurde nur ein Interview durchgeführt, somit konnte bei der

Auswertung auf die Anwendung eines Kategoriensystems verzichtet werden. Die Auswertung erfolgte manuell.

3.3.2 Analyse der Daten

Bei der befragten Person handelte es sich um einen 50jährigen Insassen einer Justizvollzugsanstalt. Er stammte aus der Nähe von Bukarest und hatte zwei Kinder. Nach dem Besuch der Hauptschule habe er den Beruf des Kochs erlernt, später auch noch das Handwerk eines Schlossers. Da er in seinen gelernten Berufen in Rumänien nicht ausreichend Geld habe verdienen können, um seine Familie zu versorgen, habe er im europäischen Ausland nach Arbeit gesucht. Als Koch habe er in Rumänien umgerechnet höchstens 700 € bekommen, als Familie mit zwei Kindern benötige man monatlich jedoch etwa 1.500 €. Mit 27 Jahren sei er zum ersten Mal ins Ausland gekommen. Er sei bereits mehrere Male aus Rumänien fortgegangen. Wieder gekommen sei er immer, wenn er im Ausland auch keine Arbeit mehr gefunden habe. Mit Anfang zwanzig sei er in Rumänien wegen Einbruchs ins Gefängnis gekommen.

Vor seiner Festnahme in einer deutschen Stadt sei er erstmals auf Skimming angesprochen worden. Er sei bereits seit einigen Jahren „Casinospieler“ (siehe Transkript § 7, Seite 95) gewesen und habe sich an diesem Abend gemeinsam mit seinem Bruder im Casino aufgehalten. Beim Glücksspiel habe er verloren und daher kein Geld mehr gehabt. Da seien zwei rumänische Staatsangehörige auf sie zugekommen und hätten gefragt, ob sie für einen Abend Arbeit 2.000 € verdienen wollten. Dieses Angebot habe man nicht ablehnen können. Man habe von diesen Personen einen „Scanner“ und eine Kamera sowie genaue Anweisungen erhalten und habe daraufhin den Geldautomaten manipuliert. Beim späteren Abnehmen der Technik sei man festgenommen worden. „*Das war die ganze Geschichte*“ (siehe Transkript § 8, 95).

In Rumänien sei er selbst nicht mit Skimming in Kontakt gekommen. Aber in Rumänien wisse man, dass man damit schnell Geld verdienen könne: „*All diese Jungs, die so gut im Internet und Computer sind, alle machen so was*“ (siehe Transkript § 11, Seite 95). Weiter führte er aus, dass in der Justizvollzugsanstalt, in der er sich zum Zeitpunkt des Interviews befand, kein weiterer Skimming-Täter einsäße. „*In Rumänien, wenn ich gewesen wäre, hätte ich*

Ihnen viel mehr helfen können. Denn von hundert Leuten fünfzig beschäftigen sich mit diesen Dingen“ (siehe Transkript § 14, Seite 95).
Der Befragte gab an, seine Ausbildung habe keine Inhalte aus den Bereichen Elektrotechnik oder Informatik umfasst. Dies habe sich geändert: „*Aber jetzt schon, diese Jugendlichen lernen das alle*“ (siehe Transkript § 15, Seite 95). Er führte hierzu aus, dass ihm zwei Personen bekannt seien, die für eine sehr gute Bezahlung von amerikanischen Unternehmen angeworben wurden.
Allgemein gefragt, wie er sich im Ausland zurechtgefunden habe, gab er an, sich zuerst eine Pension gesucht zu haben. Sodann habe er Kontakt mit anderen rumänischen Staatsangehörigen aufgenommen, damit diese ihm ein günstigeres Zimmer organisieren konnten. „*Also wenn ich ein Problem habe, gehe ich und suche einen Rumänen. Mit dem verständige ich mich und er erklärt mir, was ich tun kann*“ (siehe Transkript § 20, Seite 95). Die Sprache sei dabei ein elementarer Aspekt: „*Naja, man geht zu einem, mit dem man reden kann. Und nicht zu einem, mit dem man sich nicht verständigen kann*“ (siehe Transkript § 20, Seite 95). Sein Bruder lebe mit seiner Familie in Italien. In Italien könne man sich aufgrund der sprachlichen Verwandtschaft gut verständigen, „*sechzig Prozent ist gleich*“ (siehe Transkript § 20, Seite 95).
Hinsichtlich der wirtschaftlichen Lage in Rumänien gab der Befragte noch an, dass er sich in einer deutschen Stadt über die Verkaufspreise von Wohnhäusern gewundert habe. Die Preise seien billiger gewesen, als in Rumänien (siehe Transkript § 18, Seite 95).

4. Diskussion der Forschungsergebnisse

Die gewonnen und in Kapitel 3 dargestellten Forschungsergebnisse sollen im Folgenden diskutiert und miteinander abgeglichen werden. Dabei erfolgt zu erst ein Abgleich der Ergebnisse aus den unterschiedlichen Erhebungsmethoden. Sodann werden im Hinblick auf die forschungsleitende Frage zwei Hypothesen aufgestellt.

4.1 Parallelen und Gegensätze

Alle Täter waren männlich. Eine Aussage zum Geschlecht der Täter im Allgemeinen kann daraus nicht geschlossen werden, da die Grundgesamtheit zu gering ist. Dies gilt auch für die nachfolgenden Faktoren. Ausgehend vom Familienstand der jeweiligen Täter ergeben sich keine Auffälligkeiten. Die Täter waren zwischen 20 und 49 Jahren alt und lebten – zumeist entsprechend des jeweiligen Alters – alleine bzw. waren verheiratet und hatten Kinder. Auch die Betrachtung des jeweils höchsten Bildungsabschlusses lässt keine Besonderheit erkennen. Auch wenn die Grundgesamtheit von neun Tätern für eine quantitative Auswertung zu klein ist, kann hier von einer gleichmäßigen Verteilung gesprochen werden. Weder sind auffällig viele der Täter ohne bzw. mit geringer Schulbildung, noch finden sich vergleichsweise viele mit hohen Bildungsabschlüssen.

Auffallend ist, dass sich nahezu alle Täter in einer finanziell problematischen Lage befanden, in Teilen kam die mangelhafte Absicherung durch das Sozialsystem hinzu. Hinzu kommt, dass nach Auswertung der Ermittlungsakten bei allen neun Tätern von Läufern auszugehen ist. Hier drängt sich die Frage auf, ob die finanziell schwierige Lage der Täter 1 bis 9 ausgenutzt wurde, um dies – mit dem Versprechen „ohne Risiko“ schnell, viel Geld verdienen zu können – zum risikobehafteten Anbringen der Skimming-Technik zu bewegen. Die befragten Experten führten zu diesem Aspekt den Begriff der „*Maultiere*“ (beispielsweise Experte 1, Antwort zu Frage 3, S. 105) ein. Dies sind Bandenmitglieder „niederen Ranges“, die zur Manipulation der Geldautomaten oder zu Zwecken der Geldwäsche eingesetzt werden: „*Newcommers or very poor people* (…) *are willing to assume the risks*“ (Experte 3, Antwort zu Frage 13, Seite 113). Die Rekrutierung könne dabei in einer Bar erfolgen (Experte 2, Antwort zu Frage 13, Seite 108). So erging es auch dem befragten Insassen. „*Es war in einer Bar, wo Rumänen auch waren*“, „*ich hatte verloren im Casino, ich hatte kein Geld mehr*“ (siehe Transkript § 8, Seite 95). Durch die Spielsucht hatte er sein Geld verloren und wurde in einer Bar von einem „Landsmann“ angesprochen, ob er nicht an einem Abend 2.000 € verdienen wolle; „*alles andere hat mich auch nicht interessiert. Ich wollte doch*

das Geld haben, sonst nichts“ (siehe Transkript § 12, Seite 95). Noch am gleichen Abend wurde er verhaftet.

Im Interview mit dem Insassen wurde die Bedeutsamkeit von Sprachkenntnissen thematisiert: „*man geht zu einem, mit dem man reden kann. Und nicht zu einem, mit dem man sich nicht verständigen kann*“ (siehe Transkript § 20, Seite 95). Die rumänische Sprache gehört zu den romanischen Sprachen, ebenso wie Spanisch, Portugiesisch, Französisch und Italienisch. Die bulgarische Sprache hingegen ist der südslawischen Gruppe zuzuordnen. Nochmals unterteilt nach ost- und westsüdslawisch gehören hierzu unter anderem die Sprachen Mazedonisch, Slowenisch, Kroatisch, Bosnisch und Serbisch. Auch die Täter in den analysierten Ermittlungsakten wurden von Personen gleicher Herkunft angeworben bzw. angeleitet.

Ein Abgreifen der Kartendaten sowie der dazugehörigen PIN ist ohne entsprechende Technik nicht möglich. Die Auswertung der Ermittlungsakten, insbesondere die darin befindlichen Auswerteberichte der Polizeibehörden, zeigten die Hochwertigkeit der Skimming-Technik auf. In allen Fällen haben die Täter die jeweilige Technik zur Verfügung gestellt bekommen, so auch der befragte Insasse. Experte 2 – Sachverständiger für „Cybersicherheit“ an der ULSIT – führte zur Herstellung der Technik aus: “*In most cases, people who produce skimming devices are electronics engineers or technicians with great experience in the production of electronic de-vices. Skimming devices often are produced by a team of specialists in electronics, software, computers and communications*”[54] (Experte 2, Antwort zu Frage 10, Seite 108).

Der Abgleich der verschiedenen Untersuchungsergebnisse zeigt viele Parallelen und Übereinstimmungen. In manchen Bereichen ergänzen sich die gewonnenen Ergebnisse. Insofern kann die Gesamtheit der Erkenntnisse zur Hypothesenbildung dienen.

4.2 Hypothesenbildung

Im Verlauf dieser vorwiegend qualitativ ausgerichteten Arbeit wurden diverse mögliche Motivlagen bzw. Erklärungsansätze für die Begehung von Skim-

[54] *In den meisten Fällen sind die Personen, die Skimming-Equipment herstellen, Elektroingenieure oder Facharbeiter mit großer Erfahrung in der Herstellung elektronischer Bauteile. Skimming – Equipment wird oft von einem Team verschiedener Spezialisten gebaut. Diese sind aus den Bereichen: Elektronik, Software-Programmierung, Computer und Kommunikation.*

ming-Straftaten angerissene. Diese sollen im folgenden dargestellt und kritisch geprüft werden. Grundsätzlich muss hierbei – den Erkenntnissen der Untersuchung folgend – eine Unterteilung der forschungsleitenden Frage in zwei Aspekte erfolgen: zum einen hinsichtlich der Läufer, zum anderen hinsichtlich der grundsätzlichen Entwicklung und Etablierung von Skimming-Straftaten bei bulgarischen und rumänischen Staatsangehörigen. Demnach lautet Frage eins: Warum werden Geldautomaten nahezu ausschließlich von Läufern aus Bulgarien oder Rumänien ausgeführt? Frage zwei: Warum bestehen Skimming-Gruppierungen vorwiegend aus bulgarischen und rumänischen Staatsangehörigen?
Darüber hinaus gibt es weitere Faktoren, denen eine Auswirkung auf die Begehung Skimming-Straftaten zugeschrieben werden kann, deren Erkenntnisgehalt jedoch nicht zur Hypothesenbildung ausreicht.

4.2.1 Rekrutierung der „Läufer"

Durch die drei angewandten, empirischen Methoden konnten Erkenntnisse zu sogenannten Läufern gesammelt werden. Eine solche Bezeichnung findet sich beispielsweise auch im Deliktsfeld Rauschgift: „*Der `Kern´ des Clubs habe gewusst, dass er mit Drogen handelte, sagte der Kronzeuge aus. Er habe für den Verkauf seine `Läufer´ gehabt*" (Märkische Allgemeine Zeitung 2013). So heißt es in einem Zeitungsartikel über die Festnahme eines Rockers wegen des Verdachts der Begehung von Betäubungsmittelkriminalität. Drogenkriminalität. Beim Handel mit Rauschgift muss eine große Zahl von Endabnehmern mit den gewünschten Betäubungsmitteln beliefert werden. Dieser Verkauf birgt ein hohes Risiko, da er zumeist in der Öffentlichkeit stattfindet und der Käufer und Verkäufer persönlich miteinander in Kontakt treten. Da dies zu einem erhöhtem Festnahme- bzw. Wiedererkennungsrisiko führt, lassen Rauschgiftbanden diese Tathandlung von Läufer ausführen. Ebenso verhält es sich beim Skimming. Betrachtet man den gesamten Ablauf eines Skimming-Vorganges, so finden lediglich drei Schritte in der Öffentlichkeit statt: Montage sowie Demontage der Skimming-Technik und der Einsatz der Kartenfälschungen zum Cashing. Insbesondere das Anbringen und das spätere Abnehmen der Skimming-Technik beinhalten eine hohes Risiko,

festgenommen zu werden. Insofern stellt sich die Frage, wie ebendiese Läufer rekrutiert werden und welche Motivlage die jeweiligen Personen leitet.

Die Suche nach Läufern findet, den Untersuchungsergebnissen folgend, sowohl in den Herkunftsländern Rumänien und Bulgarien statt, als auch in Deutschland. Bei der Suche in Deutschland (oder anderen Ländern außerhalb Rumäniens bzw. Bulgariens) werden gezielt Personen gleicher Staatsangehörigkeit angesprochen. Dies ist im Hinblick auf die sprachliche Verständigung zu erklären. Neben der Sprache weckt aber auch allein das Gefühl, im fremden Ausland eine Person gleicher Herkunft zu treffen, Vertrauen. In den meisten Fällen drängte eine finanziell unausgeglichene Lage die späteren Läufer dazu, Skimming-Straftaten zu begehen. Zumal die – in Aussicht gestellte – Bezahlung sehr lukrativ schien. Die Ergebnisse aller drei Methoden liefern hierzu folgende Schlagwörter: Arbeitslosigkeit bzw. schlechte finanzielle Vergütung in den Heimatländern und fehlende bzw. unzureichende Sozialsysteme.

Schätzungen des Internationalen Währungsfonds (IWF)[55] zufolge, lagen die Länder Bulgarien und Rumänien im Vergleich des Bruttoinlandsproduktes pro Kopf im Jahr 2013 in der unteren Hälfte auf den Plätzen 79 und 72; Deutschland lag auf Platz 18 (International Monetary Fund 2013).
Betrachtet man die Entwicklung des Bruttoinlandsproduktes der Länder Bulgarien und Rumänien über den Zeitraum 1980 bis 2013 im Vergleich zur Gesamtentwicklung Osteuropas[56], können im groben Verlauf keine Besonderheiten ausgemacht werden (siehe Anlagen, Seite 118).
Die Bundeszentrale für politische Bildung veröffentliche Zahlen von Eurostat, wonach die Arbeitslosenquote im Jahr 2012 in Rumänien 7,0 % und in Bulgarien 12,3 % betrug; im Vergleich hierzu: Deutschland 5,5 %, Durchschnitt Europäische Union 10,5 %):

[55] Englisch International Monetary Fund (IMF)
[56] Albanien, Belarus, Bosnien und Herzegowina, Bulgarien, Kroatien, Tschechien, Estland, Mazedonien, Ungarn, Kosovo, Lettland, Litauen, Moldawien, Montenegro, Polen, Rumänien, Russland, Serbien, Slowakei, Slowenien, Ukraine

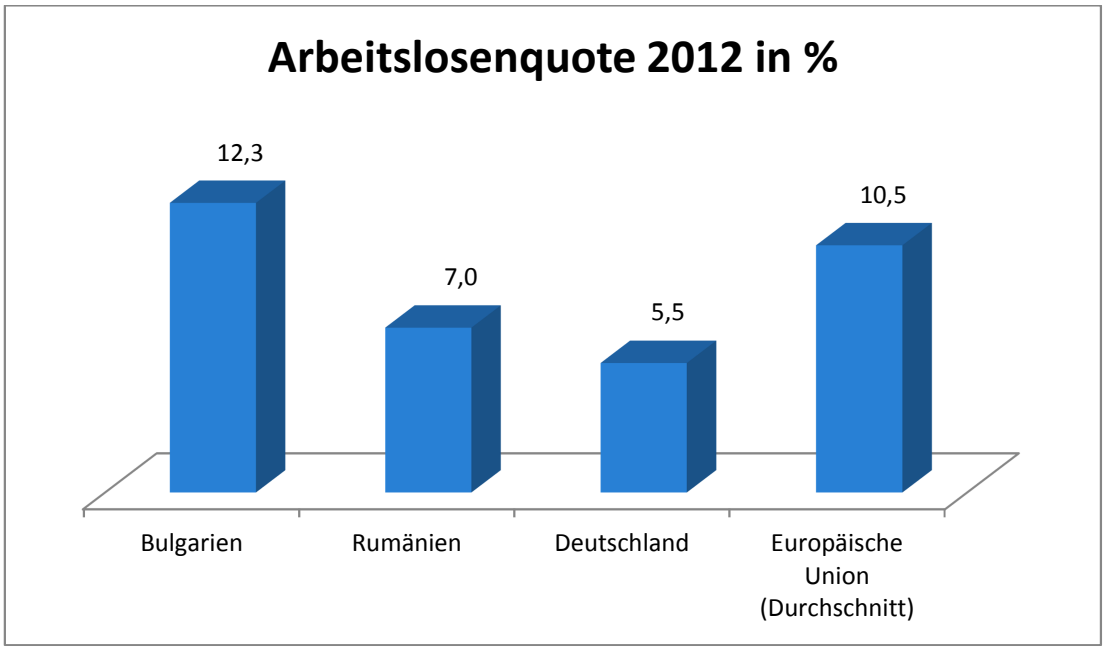


Abbildung 8: Arbeitslosenquote für das Jahr 2012 in %
(Bundeszentrale für politische Bildung 2013)

Während die Arbeitslosenquote in Rumänien unter dem europäischen Durchschnitt liegt, ist diese in Bulgarien höher als der europäische Vergleichswert. Hierbei muss angefügt werden, dass die Arbeitslosenquote in Bulgarien im Vergleich zum Vorjahr (2011) um 8,8 % gestiegen und in Rumänien um 5,4 % gesunken ist. Die durchschnittliche Arbeitslosenquote in Europa ist um 8,2 % gestiegen. Bulgarien läge somit etwas über dem europäischen Trend und die Lage der Arbeitslosenquote in Rumänien ist besser als im europäischen Vergleich. Deutlich wird, dass sich beide Länder in diesem Punkt unterscheiden, wenngleich Rumänien im europäischen Vergleich keine Spitzenwerte vorzeigen kann. Insofern kann das Merkmal Arbeitslosigkeit allein nicht ausschlaggebend sein, es kann lediglich verstärkend wirken.
Weiterhin wertete die Bundeszentrale für politische Bildung Eurostat-Daten hinsichtlich der Armutsgefährdung in Europa – vor und nach dem Bezug von Sozialleistungen aus. Angegeben wird die Reduzierung der Armutsgefährdungsquote[57] durch die Sozialleistungen des jeweiligen Landes in Prozent

[57] Die Armutsgefährdungsquote gibt an, wie hoch der Anteil der armutsgefährdeten Personen an einer Gesamtgruppe ist. Als armutsgefährdet gelten Personen, deren Einkommen weniger als 60 Prozent des mittleren Einkommens beträgt. Dabei berücksichtigt die Einkommensberechnung sowohl die unterschiedlichen Haushaltsstrukturen als auch die Einspareffekte, die durch das Zusammenleben – durch gemeinsam genutzten Wohnraum, beim Energieverbrauch pro Kopf oder bei Haushaltsanschaffungen – entstehen. Die Einkommen werden also gewichtet (Bundeszentrale für politische Bildung 2011).

(für das Jahr 2008). Im europäischen Durchschnitt wird die Armutsgefährdungsquote durch Sozialleistungen im Durchschnitt um 35,1 % gesenkt. Dagegen erfolgt in den Ländern Bulgarien und Rumänien lediglich eine Absenkung um 17,4 % bzw. 23,0 % (Bundeszentrale für politische Bildung 2011)[58]. Damit liegen die beiden Länder auf dem vorletzten bzw. letzten Platz. Bleibt die Frage, weshalb Straftäter anderer Länder, wie etwa die des Baltikums, nicht auf die Möglichkeit der Geldbeschaffung durch Skimming-Straftaten zurückgreifen. Mit nur einer Absenkung um 15,2 % und einer Arbeitslosenquote von 14,9 % liegt Lettland beispielsweise noch hinter den Ländern Bulgarien und Rumänien zurück. Auch für Litauen und Estland sehen die Zahlen nicht wesentlich besser aus.
Ein rein ökonomischer Erklärungsansatz (fehlende/nicht ausreichend bezahlte Arbeit, hohe Kosten durch Krankheitsfälle, schlechte Sozialsysteme, etc.) greift an dieser Stelle zu kurz. Fehlende Mittel zur Erreichung gesellschaftlicher Ziele im Sinne der Anomietheorie können zwar Kriminalität, aber kein bestimmtes Delikt, erklärbar machen.

Die im Laufe der Untersuchung gewonnen Erkenntnisse deuten darauf hin, dass bei der Auswahl durch die „Hintermänner“ [59] einer Skimming-Gruppierung gezielt Personen aus dem Heimatland der Skimming-Gruppierung angesprochen werden. Da die Gruppierungen nahezu ausschließlich in Bulgarien und Rumänien ansässig sind – näheres hierzu wird unter Punkt 4.2.2 thematisiert – werden für die risikoreichen Aufgaben bulgarische und rumänische Staatsangehörige gesucht. Eine gemeinsame Sprache ist zum einen Grundvoraussetzung für Verständigung, zum anderen schafft die gemeinsame Herkunft und eine ähnliche Sozialisation im gemeinsamen Heimatland Vertrauen: „*Also wenn ich ein Problem habe, gehe ich und suche einen Rumänen. Mit dem verständige ich mich und er erklärt mir, was ich tun kann*“ (siehe Transkript § 20, Seite 95), so der befragte Insasse, der rumänischer Staatsangehöriger ist. „*Naja, man geht zu einem, mit dem man reden kann. Und nicht zu einem, mit dem man sich nicht verständigen*

[58] Siehe Anlagen, Seite 93
[59] In diesem Zusammenhang sind mangels Einblicken in die Organisationsstrukturen von Skimming-Gruppierungen mit dem Begriff Hintermänner alle Skimming-Täter gemeint, die in der Hierarchie oberhalb der Läufer anzusiedeln sind.

kann“ (ebenda). Wird nun eine Person aus dem gleichen Heimatland, Bulgarien oder Rumänien, angesprochen, so ist diese – etwa im Sinne der erwähnten Anomietheorie – eher bereit, eine Straftat auszuüben, wenn sie sich in einer misslichen Lage befindet. Die Aktenanalyse sowie die Befragung des Insassen zeigten, dass die späteren Läufer ihre Heimatländer überwiegend aufgrund der schlechten Arbeitsmarktsituation verlassen hatten, um im europäischen Ausland Geld verdienen zu können. Da dies nicht allen gelang bzw. nicht durchgängig Arbeit im Ausland gefunden werden konnte, befanden sich die Personen wiederum in einer misslichen finanziellen Lage und gingen insofern auf die lukrativen Angebote ihrer „Landsmänner“ ein. In einer anderen Fallgestaltung waren die Personen bereits im Heimatland angesprochen und von Gewinnaussichten gelockt worden. In einem unter Punkt 2.2 erwähnten Urteil des BGH führte der 3. Strafsenat aus: „*Auch das Tatinteresse der Angeklagten war hoch; denn der Umfang der ihnen zum Teil gezahlten und im Übrigen versprochenen Entlohnung mag zwar nach herkömmlichen mitteleuropäischen Maßstäben eher gering erscheinen; das Entgelt hätte den Angeklagten jedoch in ihrer Heimat für mehrere Monate zum Leben genügt*“ (BGH, Urteil vom 27.02.2011, 3 StR 419/10).

Insofern ist grundsätzlich zu konstatieren, dass die Läufer von ökonomischen Beweggründen getrieben schienen. Das Risiko, eine Skimming-Straftat zu begehen, wird durch eine missliche finanzielle Lage erhöht. Hierbei handelt es sich aber um breit anwendbare Aussagen. Hinsichtlich der Frage, weshalb in den überwiegenden Fällen nur Läufer bulgarischer oder rumänischer Staatsangehörigkeit festgenommen werden, kann als Konsequenz aus den dargestellten Untersuchungsergebnissen folgende Hypothese aufgestellt werden:

Skimming-Gruppierungen bestehen nahezu ausschließlich aus bulgarischen bzw. rumänischen Staatsangehörigen. Die Gruppierungen suchen gezielt nach Mittätern, die aus dem jeweiligen Heimatland stammen. Die gemeinsame Sprache bildet die Basis für eine Verständigung. Die gemeinsame Herkunft bildet Verständnis und Zutrauen für einander.

Somit sind überwiegend bulgarische und rumänische Staatsangehörige „Skimming-Läufer".

4.2.2 Zugang zum Tatmittel

Eine wirtschaftlich missliche Lage „befähigt" nicht zum Skimming-Experten und Skimming-Straftaten kann nur begehen, wer Zugang zum Tatmittel, dem elektronischen Equipment, hat. Diesen Zugang haben fast ausschließlich bulgarische und rumänische Staatsangehörige.

Zwei der befragten Experten erklärten spezielle Anforderungen an die Täter als ursächlich für die nahezu ausschließliche Begehung von Skimming-Straftaten durch rumänische bzw. bulgarische Staatsangehörige. Die Herstellung der Tatmittel – Skimming-Technik – erfordert "*spezifische Kenntnisse und Fertigkeiten* (…) *solche von IT-Spezialisten* " (Experte 4, Antwort zu Frage 6, Seite 116). „*The manufacturer must be a specialist in the field. He may need to import some devices already built in order to finalize the skimming device. The components are bought separately from China, England etc, usually ordered online*" (Experte 3, Antwort zu Frage 7, Seite 113). Durch Experten 2 wird eine mögliche Erklärung aufgeworfen, weshalb ebendiese Experten (fast) nur in Bulgarien und Rumänien zu finden sind: "*In the 80s of the 20th century, in Bulgaria and Romania education in computer science and Electronics was very good, also had many productions of various electronic devices.*

In the 90s, most of these industries were closed or went bankrupt, and many experts were left without work.

Some of these professionals immigrated to other countries, others changed their profession, but there are number of specialist who works for the criminals as they getting good money"[60] (Experte 2, Antwort zu Frage 6, Seite 108).

Ausgangspunkt für die verstärkte Ausbildung der Länder Bulgarien und Rumänien im Bereich Elektronik war „*das Komplexprogramm für weitere Vertie-*

[60] *In den 80er Jahren des 20. Jahrhunderts war in den Ländern Bulgarien und Rumänien die Ausbildung in den Bereichen Informatik und Elektronik sehr gut, da dort viele elektronische Waren produziert wurden. In den 90er Jahren wurden die meisten dieser Fabriken geschlossen oder gingen insolvent, sodass viele Leute arbeitslos wurden. Einige der arbeitslosen Experten emigrierten in andere Länder, andere wiederum schulten um. Aber es blieb immer noch eine gewisse Anzahl an Experten übrig, die für eine gute Bezahlung Kriminellen zuarbeitet.*

fung und Vervollkommnung der sozialistischen ökonomischen Integration der Mitgliedsländer des RGW“ (Zwass 1988, S. 84). Der Rat für gegenseitige Wirtschaftshilfe (RGW), inoffiziell auch Council for Mutual Economic Assistance (COMECON) genannt, war am 25.01.1919 gegründet worden. Gründungsmitglieder waren die damals kommunistischen Staaten UdSSR, Bulgarien, Ungarn, Polen, Rumänien und die Tschechoslowakei. Diese internationale Wirtschaftsorganisation sollte die Basis für eine Koordination der einzelnen Volkswirtschaften bilden und Spezialisierungen bzw. Kooperationen im Bereich der Produktion ermöglichen (F.A. Brockhaus 1986-1994, S. 76–77). Die wirtschaftliche Zusammenarbeit der Länder wurde hierdurch gestärkt, aber eine „*funktionsfähige Integrationsgemeinschaft*“ (Zwass 1988, S. 83) war aus diversen Gründen nicht entstanden, unter anderem fehlte es dem Exekutivorgan des RGW an Kompetenzen. Nach dem Volksaufstand in Ungarn 1956 sowie dem Prager Frühling mit seinem gewaltsamen Ende wurde die „*Wirtschaftsintegration als Voraussetzung politischen Zusammenhalts des Ostblocks auf die Tagesordnung gestellt*“ (ebenda). Nach längeren Vorbereitungen billigte eine Ratstagung im Juli 1971 das Komplexprogramm mit dem vorrangigen Ziel der engeren wirtschaftlichen Zusammenarbeit. Diese könne unter anderm durch „*planmäßige Erweiterung der internationalen Spezialisierung und Kooperation in Produktion, Wissenschaft und Technik*“ (Zwass 1988, S. 85) vorangetrieben werden. Elektronisierung und moderne Informatik war eine von fünf Hauptrichtungen, die das Komplexprogramm umfasste. Hierunter wurde insbesondere die Weiterentwicklung der Elektronik-Sparte präferiert: „*Das besondere Augenmerk des Junigipfels gilt den fortschrittlichsten Zweigen des Maschinenbaus, nämlich der Elektronik, den Mikroprozessoren und industriellen Robotern*“ (Zwass 1988, S. 136). Letztlich wurde der RGW im Jahr 1991 formell aufgelöst, die Ziele konnten größtenteils nicht umgesetzt werden, vorwiegend mangelte es an einer starken Zentralverwaltung.

Unabhängig hiervon muss ein Aspekt näher beleuchtet werden, die die „*weitreichende Nutzung der Vorteile der internationalen Arbeitsteilung und der Wirtschaftsintegration*“ (Zwass 1988, S. 158). Nach sozialistischer Lehre sollten die Volkswirtschaften keine Konkurrenz zueinander bilden, sondern sich gegenseitig fördern und ergänzen. Auch im Bereich der Elektronik (später

ebenso Informatik) entwickelten einzelne Mitgliedsstaaten Spezialisierungen. Neben der Sowjetunion investierten auch die DDR und Ungarn in den Bereich Elektronik, die Elektronisierung war schließlich Hauptaugenmerk des RGW. Für die Länder Bulgarien und Rumänien stand diese Sparte jedoch besonders im Fokus. „*Von besonderer Bedeutung sind die wissenschaftlich-technischen Ergebnisse Bulgariens in den Bereichen Elektrotechnik, Rechentechnik u.a., mit denen sich Bulgarien auf dem internationalen Markt als Lieferant und Partner durchsetzen konnte*“ (Indshowa und Stefanow 1987, S. 32). In Rumänien wurde ein „*großes Augenmerk (…) der Elektronik und Mikroelektronik* (…) *und den feinmechanischen Erzeugnissen gewidmet*“ (Zwass 1988, S. 215). Elektronische Geräte bzw. Zubehörteile umfassten einen bedeutenden Teil der Exporte Rumäniens. Bulgarien und Rumänien investierten und profitierten von den Vorteilen des RGW, etwa günstige Rohstofflieferungen aus der Sowjetunion.

Seitens der kommunistischen Regierung Bulgariens wurde nach dem zweiten Weltkrieg eine umfassende Industrialisierung in die Wege geleitet. „*Nach Albanien war Bulgarien das am wenigsten industrialisierte Land im östlichen Europa. 1944 waren noch 86 % der Erwerbstätigen in der Landwirtschaft beschäftigt*“ (Ermann 2006, S. 70). Ende der 1980er Jahre arbeiteten nur noch 23 % der Erwerbstätigen in der Landwirtschaft, Bulgarien konnte sodann als „*agrar-industrielles Schwellenland*“ angesehen werden (Ermann 2006, S. 10). Speziell zum Bereich der Elektronikbranche schreibt Ermann: „*In technologieintensiven Branchen wie Elektronik- und Pharmaindustrie gab es in der sozialistischen Phase bestens geschultes Personal*“ (Ermann 2006, S. 70).

Doch letztlich waren alle Produktionsbereiche gänzlich auf den RGW ausgerichtet und von der gegenseitigen Hilfe anderer Mitgliedsländer abhängig. Die Länder Bulgarien und Rumänien hatten sich bereits vor Gründung des RGW auf den „*Intrablockhandel*“ (Zwass 1988, S. 10) eingestellt, so betrug der Anteil des Außenhandels dieser Länder mit späteren RGW-Ländern etwa 90 %.

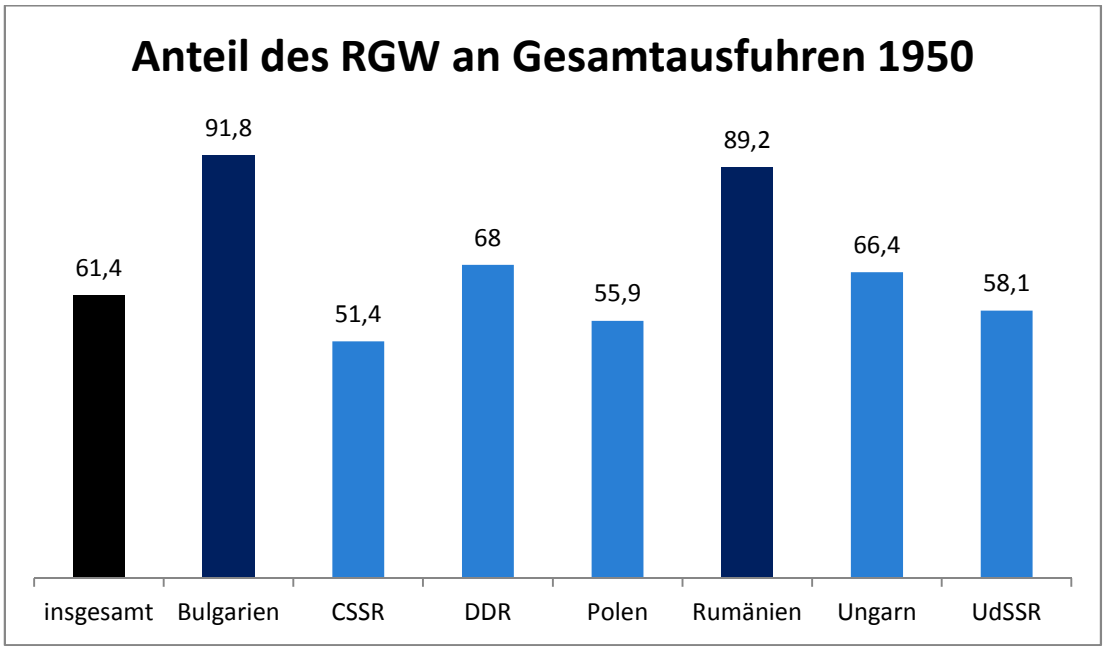


Abbildung 9: Anteil des RWG an Gesamtausfuhren 1950 in %
(Zwass 1988, S. 10)

Noch im Jahr 1989 lag der Anteil des Handels mit RGW-Ländern der Volkswirtschaft Bulgariens vom gesamten Außenhandel bei knapp 80 %: „*Durch die Auflösung des RGW wurden wichtige technologische Netzwerke blockiert* (…) *und ganze Wirtschaftszweige – wie z.B. die Elektronik oder Pharmaindustrie – kollabierten*“ (Ermann 2006, S. 51). Den bislang vor allem an die Sowjetunion gelieferten Waren und Erzeugnissen fehlte auf dem Weltmarkt jedwede Wettbewerbsfähigkeit. Erst Jahre später konnte sich diese Sparte wieder erholen. „*Dass dennoch in einigen vorher wichtigen Branchen der bulgarischen Industrie neu investiert und an die Tradition einiger alter Betriebe angeknüpft wurde, lag* (…) *an dem mit der industriellen Produktion verbundenen Humankapital*“ (Ermann 2006, S. 70). Ermann führt hierzu erklärend aus: „*generell sind der Standard der Ingenieursausbildung sowie der in der High-Tech-Produktion relevante mathematisch-naturwissenschaftliche Bildungsstand in Bulgarien im internationalen Vergleich besonders gut*“ (Ermann 2006, S. 70). Auch in der Elektroindustrie siedelten sich im Zuge der Restrukturierung ausländische Investoren an, so etwa die Firmen Kuhn Technology, Liebherr, Sparky Group, Siemens, Festo, Schneider Electric, Hyundai Engineering, ABB (InvestBulgaria Agency, S. 8).

Dieser Rückblick in die Geschichte eröffnet einen Erklärungsansatz, weshalb die für Skimming-Straftaten wichtigen technischen Kenntnisse vorwiegend in

den Ländern Bulgarien und Rumänien vorhanden sind. Es ist auch erkennbar geworden, dass es dem in diesem Bereich geschulten Personal in den 90iger Jahren des 20. Jahrhunderts an Arbeitsplätzen mangelte. Arbeitslosigkeit, Perspektivlosigkeit einerseits, besondere technische Kenntnisse auf der anderen Seite, könnten zu der Entwicklung eines bestimmten Deliktes beigetragen haben.

Seit über zehn Jahren kann die Elektronik-Branche in Bulgarien nunmehr wieder Zuwächse verzeichnen und mit den vorhandenen Fachkenntnissen werben. In dem Projekt „Promoting the advantages of investing in Bulgaria" der Bulgarischen Agentur für Investitionen[61] - mit Unterstützung durch die Europäische Union –, wurde eine Werbebroschüre erstellt. Diese Werbebroschüre soll Interessierte über die Sparte Elektrotechnik und Elektronik in Bulgarien informieren. Dabei seien folgende Merkmale für die Branche Elektrotechnik und Elektronik in Bulgarien bezeichnend: „*Verfügbarkeit von erfahrenen Ingenieuren, Qualifizierte Arbeitskräfte für den Zusammenbau von Produkten* (…) *Etablierte Traditionen in der Branche, Auf den Bedarf der Produktion gut ausgelegte Infrastruktur*" (InvestBulgaria Agency, S. 6). Das Merkmal einer traditionsreichen Branche wird dahin gehend näher erläutert, dass Bulgarien in den 70er und 80er Jahren des 20. Jahrhunderts zu „*den führenden Herstellern von elektronischen Geräten in Osteuropa*" gehört und „*in den 80er Jahren* (…) *mehr als 40 % der großen Computer-Systeme und PCs in Osteuropa*" (InvestBulgaria Agency, S. 7). geliefert habe. Mehr als 130.000 Personen waren zum damaligen Zeitpunkt in dieser Branche tätig (im Vergleich: 2010 rund 45.000 Personen), die Branche generierte mehr als 25 % der gesamten Produktion Bulgariens (InvestBulgaria Agency, S. 7, 24).

[61] InvestBulgaria Agency

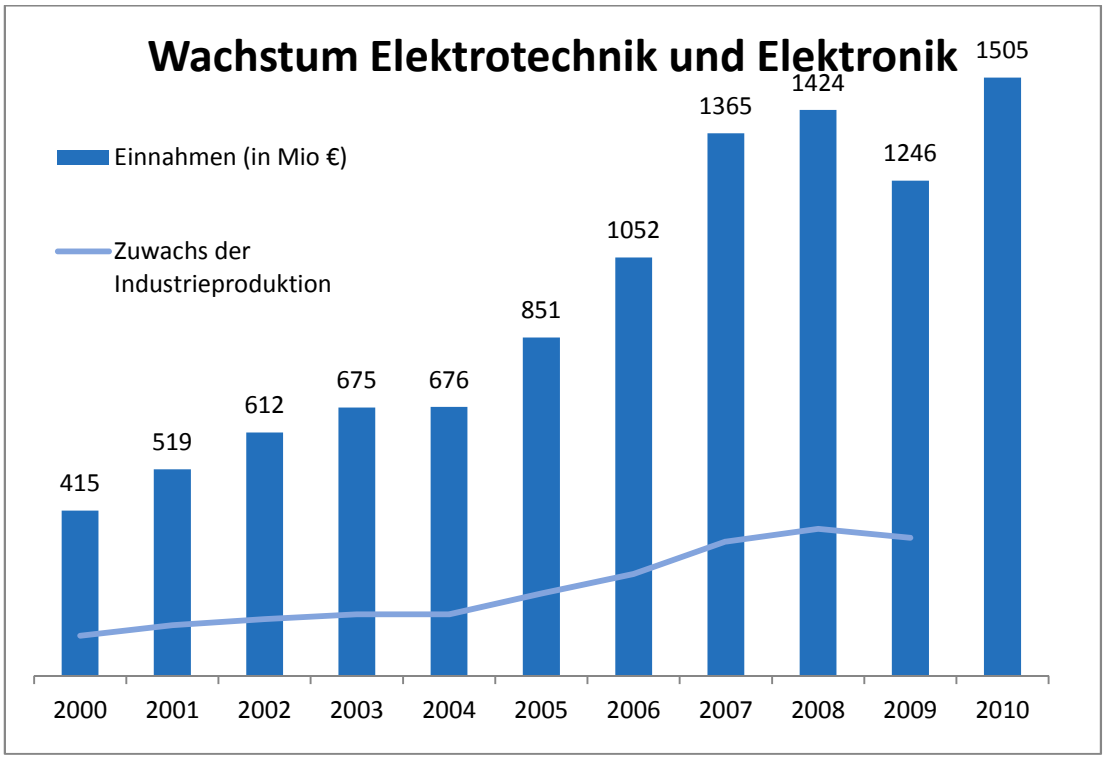


Abbildung 10: Wachstum in der Branche Elektrotechnik und Elektronik in Bulgarien nach 2000 in Mio. €
(InvestBulgaria Agency, S. 24)

Seit dem Jahr 2000 kann die Branche ein stabiles Wachstum verzeichnen. Dies hat auch Auswirkungen auf die Ausbildung in Bulgarien. „*Bulgarien bietet qualifizierte und gut ausgebildete Arbeitskräfte für den Bedarf der Branche Elektrotechnik und Elektronik an – angefangen beim Montagepersonal bis hin zu hochqualifizierten* (sic!) *Ingenieuren*“ (InvestBulgaria Agency, S. 8). Die Bulgarische Agentur für Investitionen bezieht sich auf Angaben des Nationalen Instituts für Statistik , wonach im Jahr 2010 etwa 9.000 Studenten die Fachrichtungen Elektrotechnik bzw. Elektronik studierten. Etwa 20.000 Stunden anderer Fachrichtungen suchten auf diesem Sektor nach einem Arbeitsplatz (InvestBulgaria Agency, S. 34). Neben Universitäten verfügt Bulgarien landesweit über 90 Berufsschulen, die in diesem Fachbereich ausbilden: „*Über 150 000 junge Menschen haben einen Hochschulabschluss und viele von ihnen können in der Branche eingestellt werden*“ (InvestBulgaria Agency, S. 39).

Für Rumänien liegen wenig Daten vor: „*Die deutschen Importe aus Rumänien setzten sich aus Elektrotechnik - gut ein Viertel der Einfuhren -, Kfz und*

Kfz-Teile sowie Maschinen zusammen“ (Ost-Ausschuss der Deutschen Wirtschaft 2013).

In der bulgarischen Werbebroschüre werden als jährliches Durchschnittseinkommen im Fachbereich Elektronik und Elektromaschinenbau 5.123 € angegeben (Jahr 2010). Dies liegt über dem durchschnittlichen bulgarischen Jahresverdienst im Jahr 2011 von 4.429 € (InvestBulgaria Agency, S. 41). Das europäische Portal zur beruflichen Mobilität (EURES) wertete Zahlen des Nationalen Instituts für Statistik für das Jahr 2010 aus und bezifferte die durchschnittlichen monatlichen Lebenshaltungskosten eines Haushalts auf 696,07 BGN (umgerechnet etwa 354,50 €) sowie die durchschnittlichen monatlichen Pro-Kopf-Ausgaben auf 281,59 BGN (umgerechnet 143,40 €). Dabei entfalle ein Großteil auf Ausgaben für Strom, Heizung, Wasser etc. sowie Nahrungsmittel und Getränke (EURES 2013). In Rumänien lag der durchschnittliche Nettolohn im Jahr 2011 bei 348 € monatlich (Deutsch-rumänische Industrie und Handelskammer, S. 18), also 4.176 € im Jahr. Die Lebenshaltungskosten in Rumänien beziffert EURES nicht. Es wird lediglich darauf hingewiesen, dass zwischen städtischen und ländlichen Gebieten starke Abweichungen auftreten können. Die Homepage Numbeo[62] veröffentlich diverse Preise Einzelpreise bezüglich Lebenshaltungskosten. Die durchschnittliche monatliche Miete für ein Appartement (ein Schlafzimmer) im Zentrum der Stadt Sofia beträgt demnach 253.72 €, außerhalb des Zentrums 174.23 € (Adamovic 2014). Es kann von hier aus nicht beurteilt werden, welche Werte realistisch sind. Die Bulgarische Agentur für Investitionen wirbt mit dem – für interessierte Unternehmer bedeutsamen – Hinweis: „*Es wird erwartet, dass die Löhne und Gehälter auch weiterhin noch niedrig bleiben werden*“ (InvestBulgaria Agency, S. 41). Einige Seiten weiter wird dies nochmals aufgegriffen: „*Die jungen bulgarischen Ingenieure sind hochqualifiziert (sic!), kreativ und kostengünstig*“ (InvestBulgaria Agency, S. 53). Geringere Lohnkosten im Vergleich zu anderen europäischen Ländern sollen nicht hinterfragt werden. Hinsichtlich der gesetzlichen Mindestlöhne liegen Bulga-

[62] Numbeo ist eine Datenbank, die Angaben zu Lebensbedingungen (inkl. Lebenshaltungskosten) von Städten und Ländern weltweit enthält. Die Datenbank wird – als alternative zu den offiziellen Statistiken eines Staates – von diversen privaten Quellen befüllt und nutzt somit die „Weisheit der Masse“. Die Suche nach den Parametern „Sofia“ und „Einzimmerwohnung“ basierte nach Angaben der Website auf 4.594 Einträgen der letzten 18 Monate von 259 verschiedenen Beitragenden.

rien mit 0,80 € pro Stunde (brutto) und Rumänien mit 0,97 € pro Stunde (brutto) deutlich auf den letzten Plätzen (Deutsch-rumänische Industrie und Handelskammer, S. 19). Bedeutsam wären belastbare Angaben zu den Lebenshaltungskosten, um so die Kaufkraft eines Einkommens von 5.123 € bewerten zu können. Nach Angaben des befragten Insassen benötigt eine Familie mit zwei Kindern in Rumänien monatlich etwa 1.500 € zum Leben. EUROSTAT veröffentlichte im Jahr 2012 einen Vergleich der Preisniveaus für Verbrauchsgüter und Dienstleistungen aller 27 europäischen Länder. Für das Jahr 2011 führte Dänemark die Auflistung mit dem höchsten Preisniveaus an (142 % des europäischen Durchschnitts), Deutschland lag knapp über dem Durchschnitt (103 %). Bulgarien (51 %) und Rumänien (60 %) lagen unter dem Durchschnitt. Die einzeln erfolgte Auswertung hinsichtlich des Preisniveaus von Nahrungsmitteln ermittelte für Bulgarien 67 % und für Rumänien 68 % der durchschnittlichen Preise (EUROSTAT 2012).

Ein weiterer Aspekt lässt aufhorchen. In Bulgarien werden elektronische Bauteile produziert, die Bestandteile der Skimming-Technik bilden: die „*Produktion von Printplatten (PCB) und Komponenten aus der Mikroelektronik für Industriezwecke mit weltweitem Einsatz*“ (InvestBulgaria Agency, S. 5). Darüber hinaus fertigt die Firma INCOTEX Group POS-Terminalgeräte. Die Produktionsstätten befinden sich in der Stadt Botevgrad, etwa 50 Kilometer von Sofia entfernt (INCOTEX Group 2014). Ob weitere Firmen, etwa auch Hersteller von Geldautomaten, in Bulgarien oder Rumänien produzieren, konnte nicht in Erfahrung gebracht werden. Entsprechende Herstellern gehen sehr sensibel mit Informationen um. Möglicherweise gelangen aus diesen Fabriken Informationen zu den Tätern. Allerdings gibt es verschiedene Hersteller, deren Produktionsorte nicht bekannt sind. Insofern fehlen Informationen, um diesen Aspekt weiter prüfen zu können.

Zusammenfassend kann der Elektronik-Branche in Bulgarien und Rumänien eine lange Tradition zugeschrieben werden, die durch sozialistische Wirtschaftsplanungen intensiv ausgebaut wurde und wodurch sich diese beiden Länder von anderen, aus ökonomischer Sicht aktuell vergleichbar problem-

behaftet, absetzen. Insofern kann anhand der Untersuchungsergebnisse folgende zweite Hypothese formuliert werden:

Skimming-Technik als Tatmittel limitiert den Zugang zu Skimming-Straftaten. Elektrotechnische Kenntnisse sind Voraussetzung für die Begehung solcher Straftaten. Über Jahrzehnte gewachsene Elektrotechnik-Kenntnisse speziell in den Ländern Bulgarien und Rumänien konnten nach dem Zusammenbruch der Sowjetunion nur noch bedingt in legalen Anstellungen genutzt werden. Skimming-Technik wurde entwickelt. Auch nach Erstarken der Wirtschaft und speziell der Branche Elektrotechnik im 21. Jahrhundert bleibt Skimming in Anbetracht der niedrigen Gehälter bei legaler Arbeit lukrativ. Und eine (universitäre) Ausbildung in den Bereichen Elektrotechnik und Informatik auf hohem Niveau sorgt für „Nachwuchskräfte". Somit formieren sich Skimming-Gruppierungen aus bulgarischen oder rumänischen Staatsangehörigen.

4.2.3 Ergänzende Einflussfaktoren

Im Rahmen der Untersuchung konnten weitere Faktoren festgestellt werden, die Skimming-Täter beeinflussen bzw. beeinflussen können. Diese wurden zum einen nicht als geeignet gesehen, die forschungsleitende Frage zu beantworten. Zum anderen sind diese Faktoren nur „aufgeflackert" und insofern nicht intensiv genug betrachtet worden, als dass sie Grundlage einer Hypothese sein könnten. Dennoch sollen sie Erwähnung finden.

Der Faktor „gemeinsame Sprache" ist bereits in Hypothese ein aufgegriffen worden. Dieser Faktor kann ebenfalls die Auswahl der Länder, in denen Skimming-Straftaten verübt werden sollen, beeinflussen. So ist die Verständigung für rumänische Staatsangehörige etwa in Italien oder Spanien einfacher, weshalb diese Länder möglicherweise gezielt angesteuert werden. Hierzu müsste ein Vergleich erfolgen, ob Gruppierungen aus Rumänien verhäuft romanisch-sprachige Länder auswählen und Gruppierungen aus Bulgarien dementsprechend Länder aus dem slawischen Sprachraum. Hinzu kommt die Bonität der jeweiligen Einwohner eines Landes: „*Inhaber von Zahlungskarten deutscher Emittenten verfügen im internationalen Vergleich über*

eine hohe Bonität. Daher sind deren Karten bzw. Kartendaten begehrtes Ziel von Straftätergruppierungen“ (Bundeskriminalamt 2013a, S. 5).
Zudem könnten Strafzumessung und Arbeit der Strafverfolgungsbehörden eine Rolle spielen. Experte 1 erwähnte die „*legislation*“[63] (Experte 1, Antwort zu Frage 6, Seite 105). Ein Vergleich der Strafgesetzbücher sowie eine Auswertung der jeweiligen Verurteilungsstatistiken müsste erfolgen, um hierzu eine fundierte Aussage treffen zu können.

Eine weitere Experten-Aussage scheint interessant: “*As far as I know, the gangs control the use of skimmers and battle against theirs competitors. For this reason, small bands or ´free´ criminals have no chance to carry out their activities*[64]. (Experte 2, Antwort zu Frage 8, Seite 108). Dies könnte nicht nur erklären, warum Skimming-Taten grundsätzlich von Gruppen und nicht von Einzeltätern begangen werden. Es könnte aber auch erklären, warum der Einstieg für Personen anderer Staatsangehörigkeit schwierig ist.

Ein letzter Punkt, der sich an den Ansatz der Lerntheorien annähert: “*For example, if a group of people started this kind of activities at a certain time and they remained unpunished for a long time despite the fact that theirs wealth continuesly increased over the years, determined many young people to think that this kind of activities would increase their income and that this is a way to become wealthy*”[65] (Experte 3, Antwort zu Frage 21, S. 113) Die Aussage des befragten Insassen geht auch in diese Richtung: “*In Rumänien, wenn ich gewesen wäre, hätte ich Ihnen viel mehr helfen können. Denn von hundert Leuten fünfzig beschäftigen sich mit diesen Dingen*!“ (siehe Transkript § 14, 95). Überspitzt gesagt und ohne dass der Eindruck eines Generalverdachts erweckt werden soll: Skimming als „Volks-Straftat“? Ein interessanter Aspekt, der weiter verfolgt werden könnte. So fehlen jedwede quantitativen Daten.

[63] Englisch legislation – Gesetzgebung
[64] *Soweit ich weiß, kontrollieren die Gruppierungen die Nutzung von Skimming-Equipment und „bekämpfen“ sich mit ihrer Konkurrenz. Aus diesem Grund haben kleine Gruppen oder „freie“ Einzeltäter keine Chance.*
[65] *Zum Beispiel: Wenn eine Gruppe mit dieser Art von Aktivität beginnt und für eine längere Zeit ungestraft davon kommt und zudem deren Wohlstand zunimmt, dann denken viele junge Leute, dass diese Aktivitäten ihr Einkommen erhöhen könnten und es ein einfach Weg ist, Geld zu verdienen.*

4.3 Kritik an eigenen Studien

Grundsätzlich kann gesagt werden, dass die Auswahl und das Zusammenspiel der Methoden sowie der Quellen bzw. des jeweiligen Feldes gelungen scheinen. Insbesondere im Hinblick auf die Anwendung der Triangulation konnte festgestellt werden, dass die unterschiedlichen Daten ergänzend zusammenkamen und so aus verschiedenen Perspektiven auf den Forschungsgegenstand blicken ließen.

Hinsichtlich der Inhaltsanalyse von Ermittlungsakten bleibt folgende Kritik anzumerken: Die Auswahl der analysierten Ermittlungsakten stellte keine Zufallsauswahl dar, sondern erfolgte selektiv. Die Auswahl von Ermittlungsakten der Staatsanwaltschaft Frankfurt a.M. sowie die Entscheidung, keine Akten einer weiteren Staatsanwaltschaft heranzuziehen, erfolgte aus Gründen der Praktikabilität sowie aus ökonomischen Erwägungen (Mayring 2010). Im Hinblick auf quantitative Untersuchungen ist der geringe Umfang des Materials anzumerken. Da die Analyse überwiegend qualitativ vorgenommen wurde, ist der Umfang akzeptabel. So schreibt Bude, dass einzelne Fallrekonstruktionen „*auf Gesetze des Typischen, nicht des Repräsentativen*“ abzielen (Hauptbegriffe Qualitativer Sozialforschung 2011, S. 61).
Zur Entstehung des analysierten Datenmaterials – und damit einhergehend zum Aussagewert – ist anzumerken, dass es sich um Dokumente handelt, die im Rahmen eines Strafverfolgungsverfahrens entstanden sind. In diesem Rahmen verfolgen alle Beteiligten eigene Ziele, die Strafverfolgungsbehörden, die Beschuldigten, die Rechtsanwälte. Bei den Beschuldigten ist die emotionale Belastung anzufügen.
Die Analyse bezog sich auf schriftliche Unterlagen. Die Angaben der Beschuldigten wurden protokolliert oder es wurden Stellungnahmen von Rechtsanwälten in das Verfahren eingebracht. Es handelt sich größtenteils nicht um wörtliche Aussagen der Beschuldigten. Diese Punkte wirken sich möglicherweise verfälschend aus und sind im Rahmen einer Analyse zu beachten.

Bezug nehmend auf die schriftliche Expertenbefragung muss gesagt werden: Die Auswahl der Experten erfolgte bewusst. Anzustreben ist grundsätzlich

eine Zufallsstichprobe (Schnell 1995, S. 278–279). Hierbei besteht die Problematik eines fehlenden „Verzeichnisses“ von Personen mit Expertenwissen, aus dem zufällig ausgewählt werden kann. Im vorliegenden Fall wurden einzelne Kontaktadressen bekannt. Eine Abfrage der Gesamtheit aller Personen im justiziellen Bereich (der Länder Rumänien und Bulgarien), deren Tätigkeitsbereich Skimming-Straftaten umfasst, war im Rahmen dieser Arbeit nicht zu bewältigen.
Da diese Personen an verschiedenen Orten in Rumänien bzw. Bulgarien arbeiteten und lebten, wäre es nur unter großem Zeit- und Kostenaufwand möglich gewesen, sie persönlich aufzusuchen und mündlich zu befragen. Daher wurde die Methode der schriftlichen Befragung gewählt. Eine direkte Kommunikation zwischen Fragendem und Befragten konnte hierbei nicht stattfinden. Die Methode bot demgegenüber den Vorteil, dass der Befragte in Ruhe über den Sachverhalt nachdenken und auch komplexere Antworten formulieren kann. Zudem entfällt bei geeigneter Fragestellung der Einfluss des Befragenden (Laatz 1993, S. 148–149). Aus diesem Grund wurde auch kein Telefoninterview angestrebt. Lediglich vier Personen übersandten eine Antwort. Es handelt sich somit rein mathematisch um eine positive Rücklaufquote von vierzig Prozent, dennoch bleibt eine Grundgesamtheit von vier Fragebögen. Hinsichtlich der vorwiegend qualitativen Ausrichtung dieser Untersuchung ist die zahlenmäßig geringe Menge an auswertbaren Fragebögen als noch akzeptabel eingestuft worden.

Letztlich konnte nur ein Skimming-Straftäter befragt werden. Das Vorgehen, geeignete Insassen zu finden, wurde unter Punkt 3.3.1 bereits skizziert. Die mangelnde Verfügbarkeit geeigneter Interviewpartner sollte deutlich geworden sein. Eine Anfrage an die Justizbehörden weiterer Länder war aus zeitlichen Gründen nicht umsetzbar. Dennoch wäre die Befragung weiterer Insassen wichtig gewesen, insbesondere da es sich bei der befragten Person „nur“ um einen Läufer handelte. Aus diesem Grund trat auch der Interviewleitfaden in den Hintergrund. Mit einem Pretest hätte möglicherweise eine Anpassung des Leitfadens auf Läufer bzw. Hintermänner erfolgen können. Dieser war mangels verfügbarer Personen nicht durchführbar.

Allen drei Erhebungsinstrumenten ist gemein, dass sie sich nur auf die Manipulation von beziehen, nicht auf Terminalgeräte. Dies mag dem Umstand geschuldet sein, dass Straftaten am Geldautomat derzeit (noch) häufiger auftreten. Im Hinblick auf die forschungsleitende Frage dürfte dies keine Einschränkung darstellen, da die Manipulation von Terminalgeräten als „Weiterentwicklung“ gesehen werden kann und die Gruppierungen hier auf Erfahrungen aus dem Bereich der Geldautomaten zurückgreifen.

Eine Prüfung der Hypothesen und ggf. eine Falsifizierung konnten im Rahmen dieser Untersuchung nicht geleistet werden. Die vorwiegend qualitativ ausgerichtete Methode brachte für eine Hypothesenprüfung keine ausreichenden Ergebnisse. Beispielhaft können hier die Angaben zum RGW angeführt werden. Bezüglich Bulgarien konnten diverse Daten gefunden werden, während die Angaben zur Entwicklung in Rumänien sehr spärlich waren. Grundsätzlich wäre ein Vergleich diverser Länder (nicht nur Bulgarien und Rumänien, sonder auch ökonomisch vergleichbare Länder) im Hinblick auf Ausbildungs- und Studentenzahlen, Arbeitsplätzen sowie Arbeitslosigkeit bezüglich der Elektronikbranche im Verlauf der 80er Jahre des 19. Jahrhunderts bis in das Jahr 2013 hinein wünschenswert gewesen. Diese Daten waren jedoch im Rahmen dieser Untersuchung nicht zu erlangen. Ausgehend von dem eingangs dargestellten Ziel dieser Arbeit, war eine Hypothesenprüfung nicht vorgesehen. Insofern kann diese Arbeit als „erste Annäherung“ betrachtet werden.

5. Fazit, Motivation und Ausblick

Zu Beginn dieser Arbeit stand die Frage im Raum, weshalb ein als lukrativ und risikoarm einzustufendes Delikt ausschließlich von Angehörigen zweier Nationalitäten begangen wird. Nationale Schwerpunkte in der Begehung diverser Straftaten sind nicht unüblich. Aber eine (annähernde) Ausschließlichkeit lässt aufhorchen. Der Verfasserin wurde diese Auffälligkeit in ihrer Arbeit als Sachbearbeiterin bei dem für Skimming-Delikte zuständigen Fachkommissariat des Polizeipräsidiums Frankfurt a.M. bekannt. Im Rahmen der polizeilichen Tätigkeit konnte keine Begründung gefunden werden. Das Fach-

kommissariat und der Zuständigkeitsbereich wechselten, doch die Frage blieb. Insofern schien eine empirische Untersuchung im Rahmen der Masterarbeit die geeignete Möglichkeit, eine Erklärung oder zumindest Erklärungsansätze zu finden.

Die Auswahl der Herangehensweise sowie der Untersuchungsmethoden war im Bezug auf Forschungsgegenstand und Forschungszweck zutreffend gewählt. Denn der Forschungsgegenstand war aus kriminologischer Sicht nur eingeschränkt bekannt und zur forschungsleitenden Frage gab es anfangs keinerlei Erklärungsimpulse. Somit musste eine induktive Vorgehensweise gewählt werden. Durch die Wahl verschiedener Forschungsmethoden bestand die Möglichkeit, breit gefächerte Informationen zu erhalten, unter denen bestenfalls eine Antwort auf die forschungsleitende Frage gefunden werden konnte. Es konnten zwei Hypothesen aufgestellt werden.

Zur Diskussion der Forschungsergebnisse musste die grundlegende Fragestellung zweigeteilt werden. Es stellte sich heraus, dass nicht von „der“ Skimming-Gruppierung gesprochen werden kann. Skimming-Gruppierungen sind stark hierarchisch gegliedert und insbesondere zwischen der untersten Ebene der Läufer und der darüber stehenden Kontaktpersonen klafft eine Lücke: das Risiko des „Entdecktwerdens“ und die mangelnde Einbindung in die Gruppierung. Läufer werden requiriert, um die gefährlichsten Arbeiten „outsourcen“ zu können. Dennoch kann nicht jedermann Läufer werden. Trotz allem ist es der Gruppierung wichtig, Personen gezielt anzusprechen. Vertrauensbildende Faktoren wie gleiche Sprache und Herkunft spielen hierbei eine große Rolle. So kommt es, dass Skimming-Gruppierungen nahezu ausschließlich „Landsmänner“ für die die risikobehaftete, aber dennoch bedeutsame, Arbeit auswählen. Im Verlauf einer Skimming-Straftat (angefangen mit dem Herstellen der Technik bis hin zur Sicherung des erlangten Geldes) gibt es zwei Bereiche, deren „Zugang“ erschwert ist. Dies ist zum einen das Erlangen von Kartendaten. Dieser Schritt findet in der Öffentlichkeit statt und ist somit problembehaftet, aber die Kartendaten werden benötigt. Aus diesem Grund werden Personen gesucht, denen grundlegendes Vertrauen entgegengebracht wird. Die Wahl fällt auf Personen aus dem gleichen Heimatland.

Zum anderen reguliert die Skimming-Technik den „Zugang“. Hierbei handelt es sich nicht um besonders hochwertige Elektronik, aber um ausgefeilte. Das Herstellen der Technik erfordert spezielle Kenntnisse. Und nicht nur das Herstellen. Auch das Auslesen der Daten, das Aufbereiten zur Herstellung von Kartendubletten und das Warten der Technik. Es ist nicht möglich, sich einfach ein Skimming-Gerät im Internet zu bestellen und sodann Skimming-Delikte zu begehen. Hierfür ist eine ganz bestimmte Infrastruktur, ein Netzwerk von Nöten. Die Skimming-Technik muss erst einmal an den Geldautomaten angepasst werden, die ausgelesenen Daten müssen entsprechend dem ISO-Standard eines Magnetstreifens aufbereitet werden. Sodann müssen Dubletten hergestellt und im Ausland eingesetzt werden. Das dort erlangte Geld muss seinen Weg in die Heimat finden. Für alle diese Zwischenschritte hat eine Skimming-Gruppierung ihre Spezialisten. All diese Schritte eigenständig abzubilden, wäre als Einzelperson eine zu große Herausforderung.

Vorausgesetzt, es gibt diverse Skimming-Gruppierungen aus Bulgarien und Rumänien, die über die entsprechenden Kenntnisse, Strukturen und Netzwerke verfügen – es bleibt die Frage, weshalb sich dieses Know-how nur in zwei Ländern herausgebildet hat. Auf diese zweite Frage konnte im Rahmen der Untersuchung ein interessanter Aspekt herausgebildet werden, der zur Bildung der zweiten Hypothese führte: Die Lösung könnte in der gemeinsamen wirtschaftlichen Vergangenheit beider Länder und somit in den Grundfesten des Sozialismus liegen. Das Ziel des wirtschaftlichen Aufschwungs sollte durch Spezialisierung und Aufgabenteilung erfolgen. Bei der Zuweisung der wirtschaftlichen Schwerpunkte wurde den Ländern Bulgarien und Rumänien u. a. die Sparte der Elektronik zugeteilt. Intensive Aus- und Fortbildung und hohe Investitionen ließen diesen Wirtschaftszweig erstarken und eine große Anzahl an Personen fachliche Kenntnisse erwerben. Doch mit dem Zusammenbruch des sowjetischen Systems fiel die Wirtschaft in sich zusammen. Nun entstand eine interessante Konstellation: Viele Fachkräfte stehen stehen einer geringen Anzahl an Arbeitsplätzen gegenüber. Hinzu kommt die vermehrte Nutzung des bargeldlosen Zahlungsverkehrs mittels Zahlungsarten und Geldautomaten Ende des 19. Jahrhunderts. Möglich,

dass bulgarische und rumänische Staatsangehörige in dieser Zeit ihre technische Fähigkeiten genutzt haben, um ein neues Phänomen zu entwickeln.

Eine Überprüfung der beiden Hypothesen war im Rahmen der Masterarbeit nicht möglich. Der Untersuchungsgegenstand war zu Beginn kaum bekannt. Durch die angewandten Forschungsmethoden konnten zahlreiche Informationen zusammengetragen werden. Bezüglich der forschungsleitenden Frage konnten zwei Hypothesen aufgestellt werden. Zudem wurde im Rahmen der Arbeit das weite Feld der Kriminologie deutlich.

Im Bezug auf das Delikt Skimming bleibt die Entwicklung abzuwarten. Die statistischen Zahlen lassen einen abnehmenden Trend erkennen. Fraglich ist, ob bzw. wie lange der Sicherheitsmechanismus des EMV-Chips überdauern kann. Der bargeldlose Zahlungsverkehr ist aus unserem Wirtschaftssystem und unserem Alltag nicht mehr wegzudenken. Der Schutzzweck der §§ 152a, 152b StGB liegt in der „*Sicherheit und Funktionsfähigkeit des bargeldlosen Zahlungsverkehrs* (…) *im Zahlungsverkehr werden zunehmend Zahlungskarten als Zahlungsinstrumente eingesetzt; ihre Fälschung stellt eine hohe abstrakte Gefährdung für den Zahlungsverkehr* (…) *und für das Vermögen Dritter dar*“ (Fischer 2012, S. 1056). Die dargestellten Sachverhalten lassen Findigkeit und Versiertheit der Täter erkennen. Insofern scheint auch künftig ausreichend Raum für ein „historisch gewachsenes“ und stetig weiter entwickeltes Phänomen gegeben.

Literaturverzeichnis

Das Experteninterview. Theorie, Methode, Anwendung / Alexander Bogner (Hrsg.) (2002). Opladen: Leske und Budrich.

Hauptbegriffe Qualitativer Sozialforschung. Ralf Bohnsack (Hrsg.) (2011). 3. Aufl. Opladen: Budrich.

Report on card fraud. July 2012 (2012). Frankfurt-on-Main: European Central Bank.

BDSG. Kommentar zum BDSG sowie den Datenschutzbestimmungen von TMG und TKG/ hrsg. von Kai-Uwe Plath. (2013). Köln: O. Schmidt.

Adamovic, Mladen (2014): Cost of Living in Sofia, Bulgaria. Hg. v. Numbeo. Online verfügbar unter http://www.numbeo.com/cost-of-living/city_result.jsp?country=Bulgaria&city=Sofia&displayCurrency=EUR, zuletzt aktualisiert am 02.2014, zuletzt geprüft am 20.02.014.

Bachfeld, Daniel (2007): Angriff der Karten-Kloner. Hg. v. heise online. Heise Zeitschriften Verlag GmbH & Co. KG. Online verfügbar unter http://www.heise.de/security/artikel/Angriff-der-Karten-Kloner-270934.html, zuletzt aktualisiert am 14.12.2007, zuletzt geprüft am 20.02.2014.

Bachmann, Mario; Goeck, Ferdinand (2011): "Skimming" - Eine kriminologische Betrachtung. In: *Neue Kriminalpolitik* (4), S. 153–158.

BfDI (2011): Zwei Jahre Informationspflichten bei Datenpannen. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. Bonn/Berlin (Pressemitteilung, 30/2011). Online verfügbar unter http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2011/30_InformationspflichtBeiDatenpannen.html, zuletzt geprüft am 20.02.014.

Blaser, Urs; Stauffenegger, Andreas (2011): Von der virtuellen Bankkarte zum Bargeld. In: *Schweizer Kriminalistikjournal* (15).

Bundeskriminalamt (2010): Internationale Konferenz Zahlungskartenkriminalität vom 26.-28.05.2010. Präsentation. Online verfügbar unter http://www.bka.de/DE/ThemenABisZ/Deliktsbereiche/Zahlungskartenkriminalitaet/Lagebilder/lagebilder__node.html?__nnn=true, zuletzt geprüft am 20.02.014.

Bundeskriminalamt (2011): Bundeslagebild Zahlungskartenkriminalität 2010. Hg. v. Bundeskriminalamt. Online verfügbar unter http://www.bka.de/DE/ThemenABisZ/Deliktsbereiche/Zahlungskartenkriminalitaet/Lagebilder/lagebilder__node.html?__nnn=true, zuletzt geprüft am 20.02.014.

Bundeskriminalamt (2012): Bundeslagebild Zahlungskartenkriminalität 2011. Hg. v. Bundeskriminalamt. Online verfügbar unter http://www.bka.de/nn_233866/DE/Publikationen/JahresberichteUndLagebilder/Zahlungskartenkriminalitaet/zahlungskartenkriminalitaet__node.html?__nnn=true, zuletzt geprüft am 20.02.014.

Bundeskriminalamt (2013a): Bundeslagebild Zahlungskartenkriminalität 2012. Hg. v. Bundeskriminalamt. Online verfügbar unter http://www.bka.de/nn_233866/DE/Publikationen/JahresberichteUndLagebilder/Zahlungskartenkriminalitaet/zahlungskartenkriminalitaet__node.html?__nnn=true, zuletzt aktualisiert am 2013, zuletzt geprüft am 20.02.014.

Bundeskriminalamt (2013b): Polizeiliche Kriminalstatistik 2012. Bundesrepublik Deutschland. Wiesbaden. Online verfügbar unter http://www.bka.de/DE/Publikationen/PolizeilicheKriminalstatistik/pks__node.html, zuletzt geprüft am 20.02.014.

Bundesverband deutscher Banken (Hg.) (2013): Zahlungsverkehr in Deutschland. Online verfügbar unter http://bankenverband.de/service/fakten-zahlen/zahlungsverkehr-in-deutschland, zuletzt aktualisiert am 16.09.2013, zuletzt geprüft am 20.02.014.

Bundeszentrale für politische Bildung (Hg.) (2011): Armut vor und nach Sozialleistungen. Online verfügbar unter http://www.bpb.de/nachschlagen/zahlen-und-fakten/europa/70619/armut-vor-und-nach-sozialleistungen, zuletzt aktualisiert am 30.10.2011, zuletzt geprüft am 20.02.014.

Bundeszentrale für politische Bildung (Hg.) (2013): Arbeitslosigkeit 2012. Online verfügbar unter http://www.bpb.de/nachschlagen/zahlen-und-fakten/europa/70606/arbeitslosigkeit-2012, zuletzt aktualisiert am 01.10.2013, zuletzt geprüft am 20.02.014.

Deutsch-rumänische Industrie und Handelskammer (Hg.): Rumänien. Leistungsstarker Standort. Online verfügbar unter http://rumaenien.ahk.de/fileadmin/ahk_rumaenien/Publicatii/DE/Brosura_final_2012.pdf, zuletzt geprüft am 20.02.014.

Diekmann, Andreas (2007): Empirische Sozialforschung. Grundlagen, Methoden, Anwendungen. 18. Auflage, vollständig überarbeitete und erweiterte Neuausgabe. Reinbek bei Hamburg: Rowohlt Taschenbuch Verlag.

dpa-AFX Wirtschaftsnachrichten GmbH: Datenklau am Geldautomaten: Schaden sinkt auf elf Millionen Euro. Hg. v. Frankfurter Allgemeine Zeitung GmbH. Online verfügbar unter http://www.faz.net/agenturmeldungen/unternehmensnachrichten/roundup-datenklau-am-geldautomaten-schaden-sinkt-auf-elf-millionen-euro-12726678.html, zuletzt geprüft am 20.02.014.

Dresing, Thomas; Pehl, Thorsten (2013): Praxisbuch Interview, Transkription & Analyse. Anleitungen und Regelsysteme für qualitativ Forschende. Mar-

burg. Online verfügbar unter www.audiotranskription.de/praxisbuch, zuletzt geprüft am 20.02.014.

EMVCo (2011): A Guide to EMV. Hg. v. EMVCo (Version 1.0). Online verfügbar unter http://www.emvco.com/best_practices.aspx?id=217, zuletzt geprüft am 20.02.014.

ENISA (2009): Geldautomatenkriminalität: Überblick über die Situation in Europa und die wichtigsten Regeln, um Straftaten zu verhindern. Heraklion. Online verfügbar unter http://www.enisa.europa.eu/publications/archive/atmcrime-de, zuletzt geprüft am 20.02.014.

Ermann, Ulrich (2006): Bulgarien - aktuelle Entwicklungen und Probleme. Ulrich Ermann und Margarita Ilieva. Leibniz-Institut für Länderkunde, Leipzig. Leipzig: Leibniz-Inst. für Länderkunde.

EURES (2013): Lebens- und Arbeitsbedingungen. Hg. v. Europäische Kommission. Online verfügbar unter https://ec.europa.eu/eures/main.jsp?catId=8691&acro=living&lang=de&parentId=7803&countryId=BG&living=, zuletzt aktualisiert am 10.2013, zuletzt geprüft am 20.02.014.

EURO Kartensysteme GmbH: EMV. Online verfügbar unter https://www.kartensicherheit.de/de/pub/oeffentlich/wissenswertes/sicherheitsprodukte/emv_chip.php, zuletzt geprüft am 20.02.014.

EURO Kartensysteme GmbH (Hg.): MM-Merkmal. Online verfügbar unter https://www.kartensicherheit.de/de/pub/oeffentlich/wissenswertes/sicherheitsprodukte/mm_merkmal.php, zuletzt geprüft am 20.02.014.

EUROSTAT (2012): Comparative price levels of consumer goods and services. Hg. v. Europäische Kommission. Online verfügbar unter http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Comparative_price_levels_of_consumer_goods_and_services, zuletzt geprüft am 20.02.014.

F.A. Brockhaus (1986-1994): Brockhaus Enzyklopädie. 18. Band RAD-RÜS. 19. völlig neu bearbeitete Auflage. Mannheim: F.A. Brockhaus.

Fischer, Thomas (2012): Strafgesetzbuch. und Nebengesetze. 59., Neuauflage: C.H. BECK (Beck´sche Kurzkommentare, Band 10).

Flick, Uwe (2009): Qualitative Sozialforschung. Eine Einführung. 2. Aufl. Reinbek bei Hamburg: Rowohlt Taschenbuch Verlag.

Flick, Uwe (2011): Triangulation. Eine Einführung. 3., aktualisierte Auflage. Wiesbaden: VS Verlag für Sozialwissenschaften (Qualitative Sozialforschung, 12).

Gläser, Jochen; Laudel, Grit (2010): Experteninterviews und qualitative Inhaltsanalyse. als Instrumente rekonstruierender Untersuchungen. 4. Aufl. Wiesbaden: VS Verlag für Sozialwissenschaften.

Hannich, Rainer (2007): Skimming - das Ausspähen von Bankkarten. In: *WIK* (6), S. 25–26.

heiseSecurity (2006): Schwachstellen in neuer Kreditkartengeneration. Hg. v. heiseSecurity. Online verfügbar unter http://www.heise.de/security/meldung/Schwachstellen-in-neuer-Kreditkartengeneration-108827.html, zuletzt aktualisiert am 08.03.2006, zuletzt geprüft am 20.02.014.

heiseSecurity (Hg.) (2014): Bankautomaten per USB-Stick übernommen. Online verfügbar unter http://www.heise.de/security/meldung/Bankautomaten-per-USB-Stick-uebernommen-2074773.html, zuletzt aktualisiert am 03.01.2014, zuletzt geprüft am 20.02.2014.

Helfrich, Barbara (2009): Millionen-Betrüger vor Gericht. Kontodaten abgefischt. Hg. v. Frankfurter Rundschau GmbH. Online verfügbar unter http://www.fr-online.de/main-taunus/kontodaten-abgefischt-millionen-betrueger-vor-gericht,1472862,3183224.html, zuletzt aktualisiert am 17.03.2009, zuletzt geprüft am 20.02.2014.

Hendrich, Imke (2010): Skimming-Welle: Betrug am Bankautomaten boomt wie nie. Hg. v. SPIEGEL ONLINE GmbH. Online verfügbar unter http://www.spiegel.de/netzwelt/web/skimming-welle-betrug-am-bankautomaten-boomt-wie-nie-a-736950.html, zuletzt aktualisiert am 29.12.2010, zuletzt geprüft am 20.02.2014.

INCOTEX Group (Hg.) (2014): POS Terminal systems. Online verfügbar unter http://www.incotex.bg/producttype/trade-equipment/nonfiscal-devices/pos-terminal-systems/, zuletzt aktualisiert am 2014, zuletzt geprüft am 20.02.014.

Indshowa, Zwetanka; Stefanow, Stefan (1987): Die VR Bulgarien und das Komplexprogramm des wissenschaftlichen Fortschritts der Mitgliedsländer des RGW bis zum Jahre 2000. Sofia: Verlag der Agentur Sofia Press.

International Monetary Fund (2013): World Economic Outlook Reports. Hg. v. International Monetary Fund. Online verfügbar unter http://www.imf.org/external/pubs/ft/weo/2013/02/weodata/index.aspx, zuletzt geprüft am 20.02.014.

InvestBulgaria Agency (Hg.): Elektro- und Elektronikbranche in Bulgarien. Online verfügbar unter http://www.investbg.government.bg/en/sectors/brochure-28.html, zuletzt geprüft am 20.02.014.

Kochheim, Dieter (2012): Skimming. Hintergründe und Strafrecht. Hg. v. Dieter Kochheim. Online verfügbar unter

http://www.kochheim.de/cf/doc/Kochheim-Skimming-2010.pdf, zuletzt aktualisiert am Januar 2012, zuletzt geprüft am 20.02.014.

Küch, Ulf (2010): "Skimming" - Fluch der neuen Technik oder nur Kapitulation vor innovativen Kriminellen. In: *der kriminalist* (10), S. 8–14.

Kuckartz, Udo; Dresing, Thorsten; Rädiker, Stefan; Stefer, Claus (2008): Qualitative Evaluation. der Einstieg in die Praxis. 2. Aufl. Wiesbaden: VS Verlag für Sozialwissenschaften.

Kuschling, Steffen; Schober, Bernd (2013): Skimming - Europa ist zu klein geworden. In: *MEPA-Fachjournal* (1), S. 14–21.

Laatz, Wilfried (1993): Empirische Methoden. ein Lehrbuch für Sozialwissenschaftler / Wilfried Laatz. Thun: Deutsch.

Levi, Michael: Organized fraud and organizing frauds. Unpacking research on networks and organization. In: *Criminology and Criminal Justice* 2008 (8).

Märkische Allgemeine Zeitung (2013): Rocker setzten Läufer zum Drogenverkauf ein. Kronzeuge belastet Bandidos im Drogenprozess in Berlin schwer. Hg. v. Märkische Verlags- und Druck-Gesellschaft mbH Potsdam. Online verfügbar unter http://www.maz-online.de/Brandenburg/Rocker-setzten-Laeufer-zum-Drogenverkauf-ein, zuletzt aktualisiert am 17.06.2013, zuletzt geprüft am 20.02.014.

Mayring, Philipp (2010): Qualitative Inhaltsanalyse. Grundlagen und Techniken. 11. aktualisierte und überarbeitete Auflage. Weinheim, Basel: Beltz Verlag.

Mujkanovic, Samir (2009): Kreditkartenbetrug. Erscheinungsformen, Trends und Ursachen. Hamburg: Diplomica-Verl.

Niggl, Peter (2010): Und plötzlich ist das Konto leer. In: *CD Sicherheits-Management* (3), S. 114–119.

Oppong, Marvin (2013): Skimming unter dem Datenschutzradar. c´t magazin. Online verfügbar unter http://www.heise.de/ct/artikel/Skimming-unter-dem-Datenschutzradar-1949827.html, zuletzt geprüft am 20.02.014.

Ost-Ausschuss der Deutschen Wirtschaft (Hg.) (2013): Rumänien. Wirtschaftliche Entwicklung. Online verfügbar unter http://www.ost-ausschuss.de/rum-nien, zuletzt aktualisiert am Juli 2013, zuletzt geprüft am 20.02.014.

Schmidt, Thomas (2012): "Skimming". Ermittlungsansätze zu einem relativ neuen Phänomen. In: *Deutsches Polizeiblatt* (2), S. 15–17.

Schnell, Rainer (1995): Methoden der empirischen Sozialforschung. von Rainer Schnell ; Paul B. Hill ; Elke Esser. 5. Aufl. München: Oldenbourg.

Treude, Daniela (2011): Möglichkeiten deutscher Strafverfolgungsbehörden bei der Bekämpfung des Skimmings. In: *der kriminalist* (3), S. 7–12.

Zwass, Adam (1988): Der Rat für Gegenseitige Wirtschaftshilfe 1949 bis 1987. Der dornige Weg von einer politischen zu einer wirtschaftlichen Integration. Wien: Springer.

Anlagen

Anlage 1: Übersicht der ausgewählten Aktenzeichen

Folgende Ermittlungsakten der Staatsanwaltschaft Frankfurt a.M. wurden ausgewertet und analysiert:

6310 Js 218386/10

5350 Js 225857/10

5350 Js 234320/11

5330 Js 250440/12

5330 Js 250440/12

5330 Js 215267/07

5330 Js 215267/07

5350 Js 233237/07

5350 Js 226890/07

5350 Js 226890/07.

Anlage 2: Erhebungskriterien der Aktenanalyse

Tat		
	Skimming	Zeitraum Stadt
	Cashing	Zeitraum Land
Täter	Identität	Geschlecht Geburtsjahr Geburtsort Geburtsland Staatsangehörigkeit Familienstand
	Bildung/Arbeit	Höchster Bildungsabschluss Erlernter Beruf Beruf zum Tatzeitpunkt Sozialer Hintergrund
	Kriminelle Karriere	Polizeilich bekannt gewordene Straftaten Vorstrafen gemäß Auszug BZR Weitere Straftaten nach untersuchter Tat Mittäter Festnahme
Schaden	Cashing	Anzahl geschädigter Bankkunden Schadenssumme
	Vorgehensweise	Auswahl des Tatorts Von wo wurde Gruppierung geleitet Rolle des Täters in der Gruppierung Erste Tat oder Folgetat Wurde Vorgehensweise aufgrund von „Negativerlebnissen“ angepasst Spezielles Vorgehen/Auffälligkeiten
	Verwertung	Wie gelangten die Bankdaten an den Ort des Cashing Wer führte Cashing durch Verteilung der Beute Höhe der Bezahlung
Verfahren	Spuren/Beweise	Digitalforensische Auswertung Rechtshilfeersuchen Sonstiges
	Verfahrensausgang	Angewandte Strafnormen Strafmaß Einziehung der Tatwerkzeuge Vermögensabschöpfende Maßnahmen

Anlage 3: Anschreiben Strafhäftlinge

Sehr geehrter Herr (Name),

seit 2012 studiere ich an der Universität Bochum den Studiengang Kriminologie. Inhalt des Studiums ist es, kriminelles Verhalten besser verstehen zu können. Die Kriminologie untersucht, wie Kriminalität entsteht, welche Art von Kriminalität es gibt und wie man kriminellem Verhalten vorbeugen oder es geeignet bestrafen kann.

Derzeit arbeite ich an meiner **Masterarbeit über Skimming-Straftaten**. Ich möchte gerne mehr über die Hintergründe dieser Straftaten wissen: Wie kommt ein Täter dazu, Geldautomaten zu manipulieren? Das Herstellen der Technik scheint kompliziert zu sein und auch das Erlangen von Bargeld mit Kartenfälschungen muss organisiert werden. Handelt ein Täter alleine oder eine ganze Bande? Viele Täter werden an den Geldautomaten/in den Banken festgenommen. Warum nehmen die Täter das Risiko auf sich, entdeckt zu werden?

Sie wurden zu einer Freiheitsstrafe verurteilt, weil Sie eine Skimming-Straftat begangen haben. Unabhängig von Ihrem Strafverfahren möchte ich Ihnen gerne allgemein Fragen zum Thema Skimming stellen. Ich glaube, dass Sie mir helfen können, Skimming-Täter besser zu verstehen.

Hierzu würde ich Sie gerne gemeinsam mit einem Dolmetscher in der JVA (Stadt) besuchen und mit Ihnen sprechen. In der Masterarbeit würde Ihr Name selbstverständlich nicht preisgegeben. Auch der Inhalt unseres Gespräches würde anonymisiert, so dass keine Rückschlüsse auf Ihre Person möglich sind.
Wenn Sie mir helfen und mit mir über Skimming-Straftaten sprechen möchten, teilen Sie dies bitte der JVA (Stadt) mit.

Mit freundlichen Grüßen

Anne Wonsack

Anlage 4: Interview-Leitfaden

Erklärung über Freiwilligkeit des Interviews
Hinweis auf Anonymität und Schutz der persönlichen Daten
Genehmigung der Aufzeichnung des Gesprächs

Darstellung der Masterarbeit / Zweck des Interviews

1. Persönliches

Wie alt sind Sie?

Wo sind Sie geboren und aufgewachsen?

Welchen Bildungsabschluss haben Sie?

Bitte beschreiben Sie mir Ihren Alltag in Ihrem Heimatland vor der Festnahme.
(insbesondere soziales Umfeld, Arbeit, Perspektiven etc.)

2. Skimming-Straftat

Warum verbüßen Sie eine Freiheitsstrafe?

War dies die erste Straftat, die Sie begangen haben?

Haben Sie in Ihrem Heimatland Straftaten begangen?

Wie kamen Sie dazu, Skimming-Straftaten zu begehen?
Von wem wurden Sie „angeworben“?
Hätte es Alternativen gegeben, anstatt Straftaten zu begehen?

Wie waren die Reaktionen Ihrer Familie auf Ihre Festnahme/Freiheitsstrafe?

3. Aufbau Skimming-Gruppierung

Bitte schildern Sie mir die erste Tat: Was war Ihre Rolle, wie lief das ab?
Erfolgte eine Einweisung/Anleitung?

Waren Sie Teil einer Bande/Gruppe?
Wie war die Gruppe organisiert?
Wer steuerte die Gruppe, wer war „der Boss“?

Kennen Sie andere Skimming-Banden?
Wie sind diese Gruppen organisiert?

Bitte schildern Sie mir die einzelnen Schritte einer Geldautomatenmanipulation.
Wie gelangen die Täter nach Deutschland?
Woher kommt die Technik?
Kann „jeder“ die Technik bedienen: anbringen und auslesen?
Welche Orte in Deutschland werden ausgewählt?

Wo kommen die Täter unter?

Welche Geldautomaten werden ausgewählt?

Wie gelangen die Daten an die Hintermänner?

Welchen Lohn haben Sie erhalten/wurde Ihnen versprochen?

Wie erfolgt die Bezahlung?

4. Allgemeiner Hintergrund Rumänien

Was ist zu/über Skimming-Straftaten in Rumänien bekannt?

Was erzählt man sich?

„Legende vom vielen Geld“?

Weshalb haben Sie Skimming-Straftaten begangen und keine anderen Taten?

Kennen sich in Rumänien viele Leute im Bereich Elektrotechnik und Informatik aus?

Unsere Statistiken weisen im Bereich Skimming nahezu ausschließlich rumänische und bulgarische Staatsangehörige aus. Können Sie sich das erklären?

Anlage 5: Freiwilligkeitserklärung und Vereinbarung

Erklärung über die Freiwilligkeit des Interviews

Hiermit erkläre ich, Herr ___ ___ , mich mit dem Interview unter den nachfolgenden Bedingungen einverstanden. Ich weiß, dass die Teilnahme an dem Interview ausschließlich auf meiner Freiwilligkeit beruht.

Mit der Audioaufzeichnung des Interviews bin ich:

☑ einverstanden

☐ nicht einverstanden.

Unterschrift Herr ___ ___ (interviewte Person)

Für die Übersetzung in die rumänische Sprache

den 13.02.2014

Vereinbarung

1. Die befragte Person wurde vor Beginn des Interviews über das Thema der Masterarbeit und den Zweck des Interviews informiert.
2. Die befragte Person hat dem Interview freiwillig zugestimmt.
3. Sofern mit Einwilligung der befragten Person eine Audioaufzeichnung erfolgte, wird diese nach durchgeführter Transkription durch die Interviewerin gelöscht. Ein Zugriff Dritter wird sorgsam vermieden.
4. Im Rahmen der Transkription werden Daten, die in irgendeiner Form Rückschlüsse auf die befragte Person zulassen, verändert (beispielsweise Personendaten, Haftdaten, Ortsnamen).
5. Die Interviewerin verpflichtet sich, die Ergebnisse des Interviews ausschließlich für den wissenschaftlichen Zweck der Erstellung einer Masterarbeit zu verwenden.
6. Weiterhin verpflichtet sich die Interviewerin zur Verschwiegenheit über personenbezogene Daten.

den 13.02.2014

Anne Wonsack
(Interviewerin)

(Dipl.-Psych., JVA)

Anlage 6: Transkriptionsregeln

Es erfolgte eine nahezu vollständige Transkription des Interviews. Dabei wurden in Anlehnung an Kuckartz et al. „*bewusst einfache und schnell erlernbare Transkriptionsregeln, die* (…) *den Fokus auf den Inhalt des Redebeitrages setzen*“, gewählt (Kuckartz et al. 2008, S. 27). Die Transkriptionsregeln orientieren sich am Praxisbuch Interview, Transkription & Analyse (Dresing und Pehl 2013, S. 20–22).

1. Die Transkription erfolgte wörtlich.
2. Die Beiträge wurden wie folgt gekennzeichnet: I= Interviewerin, B= Befragte Person, D= Dolmetscher, P= Psychologe.
3. Sprechbeiträge in rumänischer Sprache wurden als unverständlich gekennzeichnet (unv., rumänische Sprache).
4. Sofern eine Person den Redebeitrag einer anderen Person unterbricht bzw. wenn sich Redebeiträge überlappen, ist dies mit // gekennzeichnet.
5. Nach jedem Beitrag eines Sprechers wurde ein Absatz gesetzt.
6. Zum Zwecke der Anonymisierung wurden Eigennamen, Ortsnamen und weitere Angaben, die möglicherweise einen Rückschluss auf die Person des Befragten zulassen, entfernt. Dies ist an runden Klammern erkennbar; beispielsweise (Stadt).
7. Sprechpausen wurden mit (.) gekennzeichnet. Die Anzahl der Punkte steht dabei für die länge der Pause.
8. Seitens der Interviewerin getätigte, zustimmende bzw. die Erzählung anregende Artikulationen, wie „hmm“/“mhh“ , wurden nicht verschriftet.
9. Das Transkript enthält Zeitmarken
10. Inhaltlich zusammengehörende Fragen wurden in Blöcken dargestellt. Um ein Zitieren zu ermöglichen, wurden diese nummeriert (§ 1, § 2, etc.).

Anlage 7: Transkript des Interviews

	Einleitendes
§ 1	I: Herr (Name des Befragten), bitte erzählen Sie mir etwas zur Ihrer Person. #00:00:16-6#
	D: (unv., rumänische Sprache) #00:00:19-2#
	B: (unv., rumänische Sprache) #00:00:23-5#
	D: Ich komme aus Rumänien, in der Nähe von Bukarest. Etwa (Zahl) Kilometer von Bukarest entfernt, aus der Ortschaft (Ortsname). #00:00:29-4#
§ 2	I: Wie alt sind Sie? #00:00:34-8#
	D: (unv., rumänische Sprache) #00:00:35-4#
	B: (unv. rumänische Sprache) #00:00:36-0#
	D: 50. #00:00:37-5#
§ 3	I: Darf ich Sie Fragen, welche Schule Sie abgeschlossen haben? #00:00:42-3#
	D: (unv., rumänische Sprache) #00:00:44-2#
	B: (unv., rumänische Sprache) #00:00:48-2#
	D: Die Hauptschule, das sind in Rumänien zehn Jahre. Und dann drei Jahre Berufsschule. Da war mein Schwerpunkt Kochen. #00:01:00-2#
§ 4	B: Ich arbeite Beamte-Küche. (lacht) #00:01:02-4#
	I: Arbeiten Sie hier in der Küche? #00:01:10-1#
	B: Ja! #00:01:11-2#
	P: Ich darf Herrn (Name des Befragten) Essen jeden Tag essen. Es schmeckt sehr gut. (lacht) #00:01:15-7#
§ 5	I: In welchem Beruf haben Sie gearbeitet? #00:01:23-4#
	B: Als Koch, ja. Ja habe ich. (..) In Italien und Spanien. Aber Spanien nur ein Jahr oder so. #00:01:33-6#
	I: Haben Sie auch in Rumänien gearbeitet? #00:01:35-0#
	B: (unv., rumänische Sprache) #00:01:36-2#
	D: Ja aber nur kurz. Das wird nicht gut bezahlt, es ist kein Geld vorhanden. #00:01:42-6#
	I: Herr (Name des Befragten), wieviel Geld braucht man ungefähr, um in Rumänien zu leben? Nehmen wir an, als Familie mit zwei Kindern, für einen Monat. #00:01:50-4#
	B: Hmm 1.500 ungefähr (..) #00:01:53-1#
	I: Euro? #00:01:56-7#
	B: Ja, mit zwei Kindern. #00:01:56-7#
	I: Was hätten Sie als Koch in Rumänien gezahlt bekommen? #00:01:59-7#
	B: Bekomm ich nicht 1.500 (.) Maximum 700. #00:02:10-1#
§ 6	I: In welchem Alter sind Sie zum Arbeiten ins Ausland gegangen? #00:02:16-3#

	B: 15 Jahre ungefähr. #00:02:19-2#
	D: (unv., rumänische Sprache) #00:02:23-6#
	B: (unv., rumänische Sprache) #00:02:31-6#
	D: Also mit 27 Jahren, das war 1990. Da gab es nichts mehr in Rumänien. Aber ich bin immer wieder zurückgekommen, wenn ich keine Arbeit mehr hatte. #00:02:47-1#
§ 7	I: Wie kam es, dass Sie mit Skimming-Straftaten angefangen haben? #00:02:55-0#
	D: (unv., rumänische Sprache) #00:02:57-9#
	B: (unv., rumänische Sprache) #00:03:01-8#
	D: Ich bin, ja ich bin Casinospieler seit paar Jahren und das war auch mein Untergang. Deswegen bin ich auch im Knast gelandet, in (Stadt). #00:03:15-9#
§ 8	B: (unv., rumänische Sprache) #00:03:21-5# D: Eigentlich in (Stadt) ist alles passiert und hab ich diese Person kennen gelernt. #00:03:27-9#
	B: (unv., rumänische Sprache) #00:03:32-7#
	D: Ich hatte verloren im Casino, ich hatte kein Geld mehr. Ich war mit meinem Bruder zusammen. #00:03:35-0#
	B: (unv., rumänische Sprache) #00:03:45-3#
	D: Es war in einer Bar, wo Rumänen auch waren. Diese zwei Personen sind zu uns gekommen, zu mir und meinem Bruder. #00:03:54-1#
	B: (unv., rumänische Sprache) #00:04:02-6#
	D: Und sie haben uns gefragt, ob wir Zeit haben. Für einen Abend bekommen wir 2.000. Wie sollte man so etwas nicht akzeptieren?! #00:04:10-2#
	B: (unv., rumänische Sprache) #00:04:24-8#
	D: Er hatte gesagt: "Ich habe einen Scanner und eine Kamera. Du musst das nur in einer Bank anbringen. Ich erkläre dir, wie es geht. Und nach ein paar Stunden gehst du wieder hin und bringst es weg von dort." #00:04:23-9#
	B: (unv., rumänische Sprache) #00:04:32-3#
	D: Und ich bin genau so gegangen, so wie er es mir erklärt hat und habe es so gemacht und schwup die Polizei hat mich gefasst. (lacht) #00:04:32-0#
	I: Gleich beim ersten Mal? #00:04:34-4#
	B: Ja! (lacht) (unv., rumänische Sprache) #00:04:40-0#
	D: Als er die Geräte abnehmen wollte haben sie ihn geschnappt. #00:04:44-5#
	B: (unv., rumänische Sprache) #00:04:46-7#
	D: Das war die ganze Geschichte. #00:04:49-5#
	B: (unv., rumänische Sprache) #00:04:54-6#
	D: Ich habe die zwei Personen danach nicht mehr gesehen. Alle drei wurden wir verhaftet, wir waren zu dritt. Mein Bruder und ich waren noch mit einem zusammen. #00:05:02-5#
	I: Also gab´s kein Geld? #00:05:03-9#
	B: Keine Geld, kein Nix! (unv., rumänische Sprache) #00:05:08-

	7#
	D: Äh ich hab nicht einmal das Geld bekommen. Ich hätte es erst hinterher bekommen, wenn ich den zurückgebracht hätte. #00:05:15-9#
§ 9	I: Woher wussten Sie, was genau Sie mit dem Scanner und der Kamera machen sollen? #00:05:19-2#
	B: (unv., rumänische Sprache) #00:05:21-5#
	D: Er hat mir erklärt. Er hat mir genau gezeigt, wie ich das machen muss. #00:05:29-6#
	I: Zu welcher Bank sind Sie gegangen? #00:05:32-5#
	B: Äh (.) (Bankinstitut) #00:05:35-6#
	I: Warum? #00:05:36-8#
	B: (unv., rumänische Sprache) #00:05:48-6#
	D: Ja er hat es gesagt. Er sagte, in (Stadt) an der (Bankinstitut) sollen wir das machen. #00:06:04-2#
§ 10	I: Wie ist es in Rumänien, spricht man da über Skimming? #00:06:13-3#
	D: (unv., rumänische Sprache) #00:06:17-5#
	B: (unv., rumänische Sprache) #00:06:22-0#
	D: Ich habe in Rumänien keinen Kontakt mit denen gehabt, die sowas machen. #00:06:24-1#
	B: (unv., rumänische Sprache) #00:06:25-9#
	D: Und die Männer in (Stadt) habe ich vorher nicht gesehen. #00:06:31-8#
§ 11	I: War Ihnen bekannt, dass man mit Skimming schnell Geld verdienen kann? #00:06:37-1#
	D: (unv., rumänische Sprache) #00:06:41-7#
	B: (unv., rumänische Sprache) #00:06:44-7#
	D: Ja in Rumänien weiß man so was, ja! #00:06:46-9#
	B: (unv., rumänische Sprache) #00:06:50-4#
	D: All diese Jungs, die so gut im Internet und Computer sind, alle machen so was. (...) Eher so "Kids" sagt er eigentlich. #00:07:08-9#
§ 12	I: Was sollten Sie nach der Bank mit den Geräten machen? #00:07:12-4#
	D: (unv., rumänische Sprache) #00:07:14-7#
	B: (unv., rumänische sprache) #00:07:19-7#
	D: Nun ich hätte es am Abend zurückbringen sollen. Damit er das ablesen kann und dann Geld daraus machen kann. #00:07:24-5#
	I: Also war Ihre Aufgabe das Anbringen und Abnehmen der Teile? #00:07:29-1#
	D: (unv., rumänische Sprache) #00:07:32-1#
	B: (unv., rumänische Sprache) #00:07:40-3#
	D: Alles andere hat mich auch nicht interessiert. Ich wollte doch das Geld haben, sonst nichts. #00:07:45-0#

	B: (unv., rumänische Sprache) #00:07:50-6#
	D: Vielleicht am nächsten Tag hätte er jemand anderen gefunden, wer weiß und hätte ihn gefragt. #00:07:56-2#
	B: (unv., rumänische Sprache) #00:08:01-0#
	D: Oder er hätte mich wieder kontaktiert, damit ich es wieder mache. #00:08:06-6#
§ 13	I: Haben Sie in Rumänien Straftaten begangen? #00:08:09-2#
	D: (unv., rumänische Sprache) #00:08:15-1#
	B: (unv., rumänische Sprache) #00:08:23-7#
	D: Für so etwas habe ich keine Strafe bekommen. Das habe ich nicht gemacht. Ich wurde verhaftet wegen Einbruch vor dreißig Jahren. #00:08:23-8#
	B: (unv., rumänische Sprache) #00:08:33-1#
	D: Ich war so 22, 23. #00:08:36-7#
§ 14	I: Laut Statistiken begehen fast nur rumänische und bulgarische Staatsangehörige Skimming-Straftaten. Das ist sehr interessant. Können Sie sich vorstellen, weshalb? #00:08:56-2#
	D: (unv., rumänische Sprache) #00:09:10-9#
	B: (unv., rumänische Sprache) #00:09:30-9#
	D: Nein, ich weiß nicht, warum das so ist. Hier im Gefängnis ist sonst keiner wegen so etwas. Einer, der einen umgebracht hat und solche Sachen. Denn man fragt doch, "was hast du gemacht" und so. Aber da ist niemand dabei. In Rumänien, wenn ich gewesen wäre, hätte ich Ihnen viel mehr helfen können. Denn von hundert Leuten fünfzig beschäftigen sich mit diesen Dingen! Aber hier kann ich Ihnen leider nicht weiterhelfen. #00:09:53-8#
§ 15	I: Noch mal eine Frage zur Ausbildung// #00:10:00-8#
	B: //Ich bin auch Schweißer! (unv., rumänische Sprache) #00:10:15-0#
	D: In Deutschland habe ich auch als Schweißer gearbeitet, in (Stadt). #00:10:23-8#
	I: Hat Ihre Schulzeit und Ausbildung die Bereiche Elektrotechnik oder Informatik umfasst? #00:10:29-7#
	D: (unv., rumänische Sprache) #00:10:38-4#
	B: (unv., rumänische Sprache) #00:10:51-6#
	D: Zu meiner Zeit nicht, nein! Aber jetzt schon, diese Jugendlichen lernen das alle. Ich glaube nicht, das Rumänen da jetzt schlecht da steht. Die Amerikaner holen sich Jungs von uns! #00:10:59-7#
	B: (unv., rumänische Sprache) #00:11:16-1#
	D: Die werden dann mit Familie nach dort gebracht, damit sie weitergebildet werden können, dass sie dann für die Amerikaner arbeiten. #00:11:21-7#
	B: (unv., rumänische Sprache) #00:11:30-7#
	D: Ich kenne zwei Personen, denen 30.000 pro Monat angeboten wurde. (..) Jetzt arbeiten sie von zu Hause aus. #00:11:34-6#

	B: (unv., rumänische Sprache) #00:11:42-3#
	D: Das ist, was ich gehört habe, von diesen Personen. Die sind nur 16 und 17 Jahre alt. #00:11:47-5#
	B: (unv., rumänische Sprache) #00:11:50-4#
	D: Das sind gescheite Kinder bei uns! #00:11:54-8#
	I: 30.000 Euro pro Monat? #00:11:54-8#
	B: Dollar, Dollar. (..) So hab ich gehört. Ich weiß nicht, wie richtig ist oder nicht. Aber so habe ich gehört. #00:12:00-3#
	I: Für welches Unternehmen arbeiten die beiden? #00:12:05-4#
	B: Ich weiß nicht. (...) Also so eine große Firma, hundertprotzent. Mit Militär. Auftrag von Militär. #00:12:19-6#
§ 16	I: Kennen Sie eine Firma in Rumänien, die Geldautomaten herstellt? #00:12:28-1#
	D: (unv., rumänische Sprache) #00:12:32-1#
	B: (unv., rumänische Sprache) #00:12:36-6#
	D: So was gibt´s bei uns nicht. #00:12:37-3#
	B:(unv., rumänische Sprache) #00:12:45-4#
	D: Erst vor ein paar Jahren sind die Bankomaten bei uns erschienen. #00:12:51-4#
§ 17	I: Wenn Sie zum Arbeiten nach Deutschland oder in ein anderes fremdes Land kommen: Wie finden Sie sich zurecht, Unterkunft etc.? #00:13:05-9#
	D: (unv., rumänische Sprache) #00:13:13-1#
	B: (unv., rumänische Sprache) #00:13:15-9#
	D: Ich gehe zu einem Hotel// #00:13:16-8#
	B: //Wie heißen? Hmm, Pension! Pension, wo ist billiger! Und dann, wenn ich finden etwas weiter, wenn ich finden Leute, wenn ich kennen Leute oder so, sie können besorgen mir einer Wohnung für weniger Geld. Und dann bleiben zwei, drei Familien in diese Wohnung. Nicht allein. Zum Beispiel in (Stadt) ist billiger. Nicht, wie hier in (.) Für 300 Euro kannst du haben dort eine Zimmer. (.) Mit Küche, mit allem. #00:13:51-9# #00:14:37-3#
§ 18	B: (unv., rumänische Sprache) #00:14:07-0#
	D: Als ich in (Stadt) war, ein Appartement, also eine Einzimmerwohnung kostete 45.000 Euro, also viel weniger als bei uns in Rumänien. Wahrscheinlich zum Kauf? #00:14:09-7#
	D: (unv., rumänische Sprache) #00:14:11-5#
	B: (unv., rumänische Sprache) #00:14:27-6#
	D: Ja, zum Kauf! Es waren Wohnhäuser mit drei Ebenen, es waren diese Wohnhäuser, wo die Russen drinnen gewohnt haben. Für 45.000 haben sie die Wohnungen gekauft. Das ist billiger als in Rumänien. #00:14:37-3#
§ 19	I: Sind andere Mitglieder ihrer Familie in´s Ausland gegangen, um Arbeit zu finden? #00:14:41-6#
	D: (unv., rumänische Sprache) #00:14:46-1#
	B: (unv., rumänische Sprache) #00:14:54-0#

	D: Nun also, nur mein Bruder. Der wohnt bereits seit fünfzehn Jahren in Italien und die Kinder gehen dort in die Schule. #00:15:04-1# #00:15:33-8#
§ 20	D: (...) Dazu muss man wissen, dass die rumänische und die italienische Sprache sehr ähnlich sind// #00:15:18-1#
	B: //Ja ist gleich! Sechzig Prozent ist gleich. #00:15:22-0#
	I: Also kann man sich leicht verständigen? #00:15:23-5#
	D: Ja, ja. #00:15:24-8#
	I: Rumänisch und Bulgarisch// #00:15:33-8#
	B: //Nein, nein! Bulgarisch slawische, keine (.) #00:15:35-4#
	D: Das ist ganz verschieden. #00:15:41-8#
	B: Mit Jugoslawisch kann, oder Polnisch und Russisch. Rumänisch Latein, auch Spanisch. (.) #00:15:52-6#
	D: Also man sagt, Rumänisch ist die lebendige Sprache, die dem Latein am ähnlichsten ist. (..) Die lebendigste, lateinischste Sprache. Dann kommt Italienisch. #00:16:19-6#
	I: Bei den Skimming-Akten, die ich mir angesehen habe, sind Rumänen meist mit Rumänen und Bulgaren meist mit Bulgaren zusammengekommen? #00:16:32-9#
	D: (unv., rumänische Sprache) #00:16:43-9#
	B: (unv., rumänische Sprache) #00:16:50-6#
	D: Naja, man geht zu einem, mit dem man reden kann. Und nicht zu einem, mit dem man sich nicht verständigen kann. #00:16:53-7#
	B: (unv., rumänische Sprache) #00:17:03-7#
	D: Also wenn ich ein Problem habe, gehe ich und suche einen Rumänen. Mit dem verständige ich mich und er erklärt mir, was ich tun kann. #00:17:10-3#
	B: (unv., rumänische Sprache) #00:17:19-4#
	D: Und soweit es möglich ist, suche ich einen, der mir auch nahe steht. Also Freunde, Verwandte und so. #00:17:32-2#
§ 21	I: In einem Ermittlungsverfahren hat ein rumänischer Beschuldigter von der "Legende vom vielen Geld in Deutschland" erzählt? #00:17:50-9#
	D: (unv., rumänische Sprache) #00:18:03-4#
	B: (unv., rumänische Sprache) #00:18:05-6#
	D: So was weiß ich nicht. So was habe ich nicht gehört. #00:18:10-3#
§ 22	I: Wurden Sie vor dem Vorfall in (Stadt) bereits auf Skimming angesprochen? Also von Tätern, ob Sie helfen wollen? #00:18:26-6#
	D: (unv., rumänische Sprache) #00:18:38-6#
	B: (unv., rumänische Sprache) #00:18:40-6#
	D: Nein, da war es das erste Mal. #00:18:44-4#
	(Verabschiedung)

Anlage 8: Fragebogen in deutscher Sprache

Experteninterview / Fragebogen

Hinweise:

Sehr geehrter Teilnehmer,

aufgrund Ihrer beruflichen Tätigkeit verfügen Sie über besonderes Wissen zum Thema ATM-Skimming. Für meine Masterarbeit benötige ich genau dieses Wissen. Daher bitte ich Sie, mich an Ihren Erfahrungen teilhaben zu lassen. Die Fragen beziehen sich nicht auf konkrete Fälle, sondern auf allgemeingültige oder überwiegend zutreffende Beschreibungen. Da ein Fragebogen keine Rückfragen zulässt, antworten Sie bitte möglichst umfangreich und erklären Sie Ihre Aussagen.

Ihre Angaben werden vollständig anonymisiert.

Wenn Ihnen weitere Aspekte einfallen, die in den Fragen nicht behandelt werden, schreiben Sie diese gerne am Ende des Fragebogens auf.

Gerne können Sie die Fragen in Ihrer Muttersprache beantworten.

Vorab vielen Dank!

---

1. Bitte schildern Sie kurz, seit wie vielen Jahren Sie im Deliktsbereich ATM-Skimming arbeiten und welche Funktion Sie inne haben (zum Beispiel: Ermittlungsbeamter/Sachbearbeiter, Gruppenleiter/Kommissariatsleiter, Sachverständiger).

2. Wie ist eine ATM-Skimming-Bande organisiert?

3. Bitte schildern Sie die unterschiedlichen Aufgabenbereiche/Rollen, die es in einer solchen Bande Ihrer Meinung nach gibt.

4. Ist eine ATM-Skimming-Bande hierarchisch organisiert oder sind die Gruppenmitglieder gleichberechtigt?

5. Falls es einen „Kopf“ der Bande gibt: Von wo aus wird eine ATM-Skimming-Bande gesteuert? Sitzt der „Kopf“ in Rumänien oder Bulgarien oder reist dieser ebenfalls nach Deutschland?

6. Laut unserer Statistik begehen fast ausschließlich Täter aus Rumänien oder Bulgarien ATM-Skimming-Straftaten. Können Sie sich das erklären?

7. Wer stellt die ATM-Skimming-Devices her?

8. Stellt jede Gruppierung ihre Devices selbst her oder können diese gekauft werden?

9. Ist die Herstellung eines solchen Devices technisch anspruchsvoll?

10. Haben die Hersteller dieser Devices technische Vorkenntnisse (z.B. eine Ausbildung/ein Studium in den Bereichen Elektrotechnik, Informatik, Mechatronik)?

11. Sind Ihnen Fälle bekannt, in denen die Devices mittels 3D-Drucker hergestellt wurden?

12. Wie gelangen die Devices nach Deutschland?

13. Wie werden die Täter akquiriert, die in Deutschland Geldautomaten manipulieren?

14. Bekommen die in Deutschland agierenden Täter genaue Anweisungen oder arbeiten sie eigenständig?

15. Was passiert mit den ausgespähten Daten?

16. Wie werden die Daten aus Deutschland in das Ausland übermittelt?

17. Werden diese Daten verkauft oder von anderen Gruppenmitgliedern im Ausland verwendet?

18. Falls es einen „Kopf“ der Bande gibt: Wie gelangt das Geld zu diesem?

19. Wie werden die einzelnen Gruppenmitglieder bezahlt?

20. Unterscheiden sich Skimming-Straftäter von anderen Straftätern? Falls ja: weshalb?

21. Gibt es örtliche Schwerpunkte? Kommen beispielsweise auffallend viele Skimming-Straftäter aus einer Ortschaft/einer Stadt?

VIELEN DANK für Ihre Mühe!

Anlage 9: Fragebogen in englischer Sprache

Expert interview / Questionnaire

Remarks:

Dear participant,

due to your occupational background, you have valuable insights into ATM-Skimming. I would like to use this valuable knowledge for my master thesis. Therefore I would kindly ask you to let me be part of your experience. The following questions do not focus on specific cases but are rather generally valid or vastly applicable descriptions. Since questionnaires are not designed to question the given answer after submission, please answer as precisely as possible and explain your answers.
The information will be handled anonymously.
Should you have any remarks, please make these at the end of the questionnaire.
You are more than welcome to answer the questions in your mother tongue.

Thank you very much for your help!

1. Please, briefly describe for how many years you have been working in the field of ATM-Skimming and which position you have (for example: investigator/administrator, group manager/commissariat manager, technical expert)
2. How is an ATM-Skimming gang organized?
3. Please, describe the different tasks/roles that exist within such a gang.
4. Is an ATM-gang hierarchically organized or do equal membership rights exist in these groups?
5. If there is a „leader“ in the gang: How is an ATM-Skimming gang controlled? Is the leader located in Rumania, Bulgaria or does he/she travel to Germany?
6. According to our statistical records, the ATM-Skimming offender are almost exclusively from Rumania or Bulgaria. How could you explain this phenomenon?
7. Who manufactures ATM-Skimming devices?
8. Does every gang manufacture its own device or can they be purchased in the market?
9. Does the production of these devices require specific technical skills?

10. Do the manufacturers have prior technical knowledge (e.g.: apprenticeship/higher level studies in a technical field: computer science, electro-technics, mechanics)?
11. Do you know of any cases in which devices have been manufactured using a 3-D printer?
12. How do these devices make it across borders to Germany?
13. The most serious danger of getting caught and arrested can be seen when attaching devices to ATMs. Who do you think takes on this job? Are these experienced gang members or rather newly recruited members that are given specific instructions?
14. Do offender working in Germany receive any instructions or do they work independently?
15. What happens to the in Germany retrieved data?
16. How do data get transferred from Germany to other countries?
17. How do data get sold or how do data get used by other group members across borders?
18. If there is a gang leader: How does he receive the money?
19. How do individual members get rewarded/paid?
20. Are there differences between Skimming offender and other offender? If yes, why and what are these differences?
21. Are there specific local differences? Are there, for example, many Skimming offender localized in one particular town/city?

THANK YOU VERY MUCH FOR YOUR PARTICIPATION!

Anlage 10: Antworten Experte 1

1.
I have been working in the field of cybercrime-payment card frauds-ATM Skimming since 2002, first as a police investigator (2002-2008), and then (2009-2013) as the Head of the Regional Service for Countering the Cyber-criminality within the Brigade for Countering the Organised Criminality, [redacted], Romania.

2.
Suspects are very well organized in OCGs, having specific roles and hierarchies, in order to obtain illegal profits. Group members are interconnected with members from other gangs located inside or outside the national borders.

3.
Generally, there are leaders who control, organize and finance the activities, manufacturers of skimming devices, suspects who install the devices on ATMs and individuals who are assigned to cash out the funds from the compromised accounts using counterfeit cards. There are also "mules" recruited for money laundering purposes.

4.
Hierarchically. Sometimes there are multiple leaders and lieutenants with dedicated tasks.

5.
The OCG is controlled especially from RO, but when it is necessary the leader would travel abroad "to arrange the things".

6.
It is quite difficult to explain. There are multiple causes: economic context, EU developed payment marketplace, legislation.

7.
Individuals who possess more or less some technical skills.

8.
Devices are either purchased and modified, either bought from other accomplices.

9.
Yes, but not advanced.

10.

Yes, in general cases.

11.
No.

12.
By car-in person, by bus or via a shipping company.

13.
Individuals with low level of intelligence or in need of money.
Newly recruited members.

14.
He receives instructions.

15.
It is used to counterfeit cards or make payments.

16.
Electronically.

17.
Data is sold in order to gain profit and it is sent by electronic means.

18.
There are different ways:
- *in person (cash) – most used*
- *“mules”*
- *wired via Western Union, MoneyGram, bank accounts*

19.
- *in person (cash) – mostly used*
- *via “mules”*
- *wired through Western Union, MoneyGram, bank accounts*
- *cut off from their debts*

20.
There are a few differences.
Skimming offenders are creative, willing to take up risks, determined, proactive, dynamic, internationally minded.
Some of them were in the past common offenders of thefts, burglaries, violent acts, blackmail and/or serious crimes (drug trafficking, trafficking in human beings, car dealers, etc.)

21.

Yes, but the trend is that they are expanding within the national borders. Offenders originating from one specific town/region move to other cities (bigger cities) or get in touch with individuals from that areas.
There are a few counties where skimming is very “popular” and counties where other crimes are committed regularly (e.g.cyber frauds)
Nevertheless, their crimes increase in dimension and borders.

Anlage 11: Antworten Experte 2

1.
I am working as a technical expert and expert witness from about 7 years, I also have 3 years experience in working group in police for the prevention of crimes with a payment cards.

2.
On the basis of information from investigations and court trials in which I participated during the period 2007-2011, Bulgarian criminal groups were well and activity in strictly hierarchical structures consisting of different groups, each of its specific tasks (such as placing and security of skimmers, transportation of skimming devices, withdrawing money, and others). Also, there were groups from technical specialists for the production of the devices and for decoding the cards data recorded in skimmers, after their use.
During the same period, a very rare, we have been receiving information about the placement of the skimmer on Bulgarian territory by "free" (not controlled by criminal structures) criminals.
These cases were single and differed from other cases that they used handmade or lower-quality skimming devices.

In 2012, the situation gradually changed. The activity of the Bulgarian bands on Bulgarian territory began to diminish, however, began more frequent Romanian groups start withdrawing money on Bulgarian territory.

3.
The Bulgarian criminal groups dealing with skimming devices have good organization, their structure is very flexible, they consist of many groups, each group is specialized in one or more activities.
The essential in the organization is what; members of different groups rarely know each other and groups receive tasks via phone, chat, sms or intermediaries…

The activities of the groups are divided in such a way that one or two groups may not be able to close the circle of all the activities and carry out the crime from end to end.

In my practice I've encountered the following groups on the specialties:
Mules: pull money from ATMs and handed over to another group, Guards: muscle guarding and security mules while withdraw or carry money, also receive money from the mules and transmit them to the next group, Skimming mounters: group for mount skimming devices on ATMs and guard skimmers until it is placed on the ATM. In cases where Skimming mounters use “audio” skimmer, after mounting it on the ATM, criminals being tested skimmer with

called “test” card, to record in skimmer memory evidence which group has place it.

4.
In hierarchical terms until 2012, all groups working in the skimming field were part or chain to three criminal structures, competing with each other, each group had a leader who received the tasks and allocate the money to the group.

5.
The groups (gangs) are organised in chains (structures). Each gang has a leader who has the right to communicate with other groups or seniors in the structure.
In cases where the leader of the structures was arrested, according to their testimony, it appears that they not highest level of management, and actually they have managers and receive tasks from people that they don't know personal and have never even seen. Which means that the real organizers of skimming criminal activity remain hidden for police sources.

As far as I know most of the senior members of structures (chains) rarely travel in Germany and the European Union, most time they spend in Bulgaria.

6.
In the 80s of the 20th century, in Bulgaria and Romania education in computer science and Electronics was very good, also had many productions of various electronic devices.
In the 90s, most of these industries were closed or went bankrupt, and many experts were left without work.
Some of these professionals immigrated to other countries, others changed their profession, but there are number of specialist who works for the criminals as they getting good money.

7.
Skimming devices are manufactured in the so-called «factory». The “factories” can be different, depending on what skimming device produce.
There are skimmers manufactured in apartments and skimmers, which are produced in factories for electronics:

a/ “Ordinary” skimming devices (build from MP3 or MP4 recorders) can be assembled at apartment or garage, with the exception of the production of plastic parts for the camouflage of skimmers, when it is placed on the ATM.

b/ "Specialized" skimming devices, are designed by experts and their electronic circuit boards are made in legal factories for the production of electronic parts, by concealing their true purpose.
c/ Currently, several Chinese companies sell skimmers as card readers on the Internet. You can check this link:
http://www.cardreaderfactory.com/magnetic-stripe-readers.html

8.
Until 2013, skimming devices is produced only in the "factories", under control of gangs and senior managers of chains allocated them between the groups.

We received information rarely that some gang (group) has produced skimming device themselves (or bought) and use it to get money.

As far as I know, the gangs control the use of skimmers and battle against theirs competitors. For this reason, small bands or "free" criminals have no chance to carry out their activities.

9.
Yes! There are two main types of skimmers: the first is the so-called "Audio" skimmers, whose components are taken from a variety of devices – most commonly from MP3 and MP4 recorders.
The second type are special designed skimming devices, which are designed and manufactured exactly for ATM skimmer. In the production of a specialized skimmer are needed much knowledge concerning design and production of electronic devices and professional equipment.

10.
In most cases, people who produce skimming devices are electronics engineers or technicians with great experience in the production of electronic devices. Skimming devices often are produced by a team of specialists in electronics, software, computers and communications.

11.
I haven't known such cases. In Bulgarian 3D printers are few and the access to them is limited.

12.
Skimming devices are commonly sent in consignments, camouflaged in toys or home electronics. There also are many cases that devices are carried by people (mules), also known cases that skimming devices are carried by random tourists at the request of their friends.

Sometimes the skimmers are transported in parts, from different people and assembled on the place from technical specialist with an average level of knowledge.

13.
In my practice, I've dealt with different cases:
there have been cases in which skimming devices are mounted by amateurs, recruited in a bar,
but in most cases in which I have watched records from security cameras, the criminals that mount skimming devices are professionals, they put device for 5-6 seconds and in a way that could not be recorded their faces.
Also, I assume that in most cases the criminals doing the preliminary survey and monitor the ATMs to understand where there are cameras and how people use it.

Very rarely it is possible to identify a criminal by the record of the ATMs camera, for the following reasons: not all ATMs have an internal camera of most ATMs cameras only works when in it is placed a payment card, and also in cases where the camera is constantly working, the record store keeps records very short time (up to a week or little bit more)…

14.
I can point out statistics, but in most cases, the gangs operating with skimming devices attending countries, as a tourist and remain there no more than a month. There are some destinations such as Trinidad and Tobago, Domenican and Nigeria, were gangs used worked there Bulgarians for withdrawing money.

The bosses in the structure decide what group, where should work and instruct the leader of the group before group left. Even abroad, leaders of groups periodically make status reports of their seniors, using Skype or phone.

15.
There are various scenarios, but usually after being ousted from the ATM skimming devices, data from device is download with a laptop and sent to another group in Bulgaria or outside.
After that, the gang (for example: in Germany) received, data from payment cards skimmed in another destination.
The data is sent in a ready-to-record format for recording card devices (usually MSR).
The gangs can purchase from an electronics store, recorder and standard cards with magnetic strip, on which they are record the received data and produce so-called "white plastic".

16.
Criminals often use Skype or special file transfer programs.

17.
As far as I know, the Bulgarian gangs do not sell the data from skimming devices, they send data to more senior groups than them and receive in return other data – decoded and ready for recording on "white plastic" with which, criminals can withdraw money.

18.
There are several scenarios, such as most frequently used the following two:

1. Each withdrawing group held their part and transmits the rest of the next group or senior manager. Managers pay salaries on skimming mounting and security guys…
2. Most of the groups perform two activities: mount, keeps and removed from the ATM skimming device, then download information about recorded cards and PIN codes from it and sending all data to other group or criminals. Later, the gangs received files with ready-to-record data from payment cards, skimmed to another destination, criminal's record data to "white plastic" and withdraw money from ATMs, having retained part of the amount for them.

19.
Earnings/wages are allocated by the leader of the group, in relation to the obligations of the members in it.

20.
Yes. The gangs that dealing with crimes against payment cards have a better organization and more strictly controlled.

21.
It is difficult to give a definite answer, but statistic shows that the greater part of the "factories" are in the largest cities of the country, and in addition, gangs activity is greater in large cities.

Anlage 12: Antworten Experte 3

1.
I ve been working at the Brigade for Countering Organized Crime Craiova – Cybercrime Department for 7 years, occupying a specialist 1 position. Mostly I work as an investigator, coordinating activities in our cybercrime cases.
2.
Leader/leaders – executants – connections that are able to help (provide accomodation, transfer money etc)

3.
- *manufacture or assembly of the skimming devices;*
- *installing the skimming devices and data transfer / download;*
- *finding houses to accomodate, finding best places for installing devic es;*
- *transportation of equipment;*
- *forging cards using MSR;*
- *making withdrawals at ATMs;*
- *assuring protection for the criminal group*

4.
One's opinion counts more in these groups usually being the person who has more money and who invest in buying the skimming equipment.

5.
This may differ. Maybe the lider has been arrested in some countries and may avoid installing skimming devices there or he may want to supervise closely the group activities to maximise profit.

6.
I belive they target citizens of rich countries with more money in accounts than in Eastern Europe countries.

7.
The manufacturer must be a specialist in the field. He may need to import some devices already built in order to finalize the skimming device. The components are bought separately from China, England etc, usually ordered online.

8.
Ussualy they purchase this devices from a few manufactures from Romania or Bulgaria.

9.

Definately yes. Either he manufactures a mechanical part (housing) either he manufactures a electronics (hardware), the offender need to have advanced knowledge in the field.

10.
some have advanced studies in the field others are passionate and learned alone

11.
No. But I ve seen cases in which they used a 3 D machine (automatic lathe) to manufacture the housing of the skimming device (the ATM lips). That machine was originally designed for shoes industry.

12.
usually they transport only the skimming devices and maybe a MSR device with some credit cards/blanks.

13.
There had been cases in which liders installed skimming devices on ATMs but mostly for this job are used the newcommers or very pool people who are willing to assume the risks involved.

14.
Mostly they work independently but sometimes they may have some devices broken and ask for help to replace those devices.

15.
The exchange of data often takes place over internet

16.
- *Over internet in most of the cases (email or instant messaging)*
- *On memory stick or encrypted hard drives*

17.
They transmit data fast over Internet network (after they have obtain the credit cards numbers they send it over internet to a specific country where they are going to start the withdrawals. Sometimes they start in 2 or 3 countries simultaneously)

18.
The group liders receive their money by using different methods:
- *courier companies, concealed in toys or other devices (undeclared)*
- *transported by group members or connections (4 or more people with maximum sum allowed)*

- *some of them are still using Western Union or Money Gram to transfer money on relatives names*
- *also a part of liders prefer to buy expensive goods (luxury cars) that they carry in the native country and resell*

19.

If all the members of the criminal group have the same contribution to the acquisition of the skimming devices, they may share evenly the profit, But usually one or two of the group memebers identify themselves as the group liders. They generally have more money and they purchase the skimming devices. The group liders distibute a certain percentage of the profit obtained amoung group members, considerating their skills and effort.

20.

- *a skimming offender is mostly non-violent, chasing to obtain easy money with minimum of risk.*
- *a skimming offender is often tehnical well-prepared, having knowledge of the latest tehnologies related to skimming devices, wire-less/bluetooth tehnologies, video recording devices*

21.

Yes, there are some local differences in Romania. For example, if a group of people started this kind of activities at a certain time and they remained un-punished for a long time despite the fact that theirs wealth continuesly in-creased over the years, determined many young people to think that this kind of activities would increase their income and that this is a way to be-come wealthy.

Cities known in Romania as places originating for cybercrime offenders are Bacau, Craiova, Bucuresti, Ramnicu Valcea, etc.

The criminal groups from Romania often targeted countries like Italy, Spain, France where judicial authorities offered a weak response to Romania s judi-cial authorities or are known for easy punishments related to cybercrime phenomenon.

Anlage 13: Antworten Experte 4 (Übersetzung in die deutsche Sprache)

1.
Ich heiße [redacted] Ich arbeite als Kommissarin bei der Wirtschaftspolizei seit 14 Jahren, im Polizeirevier sowie bei der [redacted]. Ich bin zuständig für Straftaten im Bank- und Finanzsektor und solche in Verbindung mit Bankkarten und Skimming.

2.
Nach meiner Beobachtung wird das Skimming immer von einer organisierten Tätergruppe in einer streng hierarchischen Struktur, wobei die Rollen im Voraus verteilt werden und sich die unterschiedlichen Organisationsstufen untereinander nicht kennen, ausgeführt.

3.
Die Skimming-Gruppen werden von einem Anführer geführt, unter ihm stehen die Verantwortlichen für die verschiedenen Stufen. Die einen sind verantwortlich für die Anschaffung der Skimming-Gerätschaften, andere für die „Maultiere" die die Skimmer an die Bankautomaten montieren. Dritte für den Informationstransfer der geskimmten Bankkarten zu den Personen die die erhaltenen Daten verarbeiten und diese auf weiße Plastiken übertragen. Andere Personen sind für das „Auspumpen" der geskimmten Karten und Verteilung der erhaltenen Geldbeträge zuständig. Das Geld wird unter den Beteiligten nach vorher vereinbarten Prozenten aufgeteilt.

4.
Die Gruppenteilnehmer sind in hierarchischer Abhängigkeit und sind nicht gleichgestellt.

5.
Üblicherweise reist der Anführer der Gruppe nicht und befindet sich im Land. Die Kontrolle zwischen den Untergruppen und ihm erfolgt über Skype, Viber oder direkt über Telefon mit den Verantwortlichen.

6.
In der Tat sind die Skimming-Gruppen bulgarischer, rumänischer und ganz selten moldawischer Herkunft. Für die Anfertigung und Montage der Gerätschaften sowie für die Nutzung der herunter geladenen Daten sind spezifische Kenntnisse und Fertigkeiten erforderlich, solche von IT-Spezialisten, Taschendieben für die Montage und Demontage der Skimmer an den Bankautomaten, sowie auch technisch versierte Personen.

7.
Die Skimmer werden von Computer-Spezialisten mit guten technischen Kenntnissen hergestellt. Sie werden von den für den technischen Teil zuständigen Personen in der Gruppe bestellt.

8.
Nicht jede Gruppe stellt ihre Skimmer selbst her. Sie können unter Vorgabe von konkreten Parametern bei anderen Auftragnehmern bestellt werden.

9. und 10.
Ja – für die Herstellung der Skimmer sind spezifische technische Kenntnisse erforderlich.

11.
Ein solcher Fall ist uns nicht bekannt.

12.
Die Skimmer werden von „Maultieren“ über die Grenze gebracht. In Verstecken von Autos, im Gepäck über den Flughafen.

13.
In den meisten Fällen werden nur die Personen festgenommen die Skimmer montieren, es ist schwierig bis zu den Organisatoren zu gelangen.

14.
Die in Deutschland aktiven Täter sind geschult und arbeiten in den meisten Fällen nicht selbstständig. Sie sind geschult die Gerätschaften zu montieren und zu demontieren sowie diese zu reparieren im Falle eines Defekts.

15. und 16.
Nach Beschaffung von Kartendaten in Deutschland werden diese elektronisch oder mit einem mobilen Speicher nach Bulgarien oder an einen anderen Ort für Datenverarbeitung und Aufbringen auf weiße Plastiken übertragen.

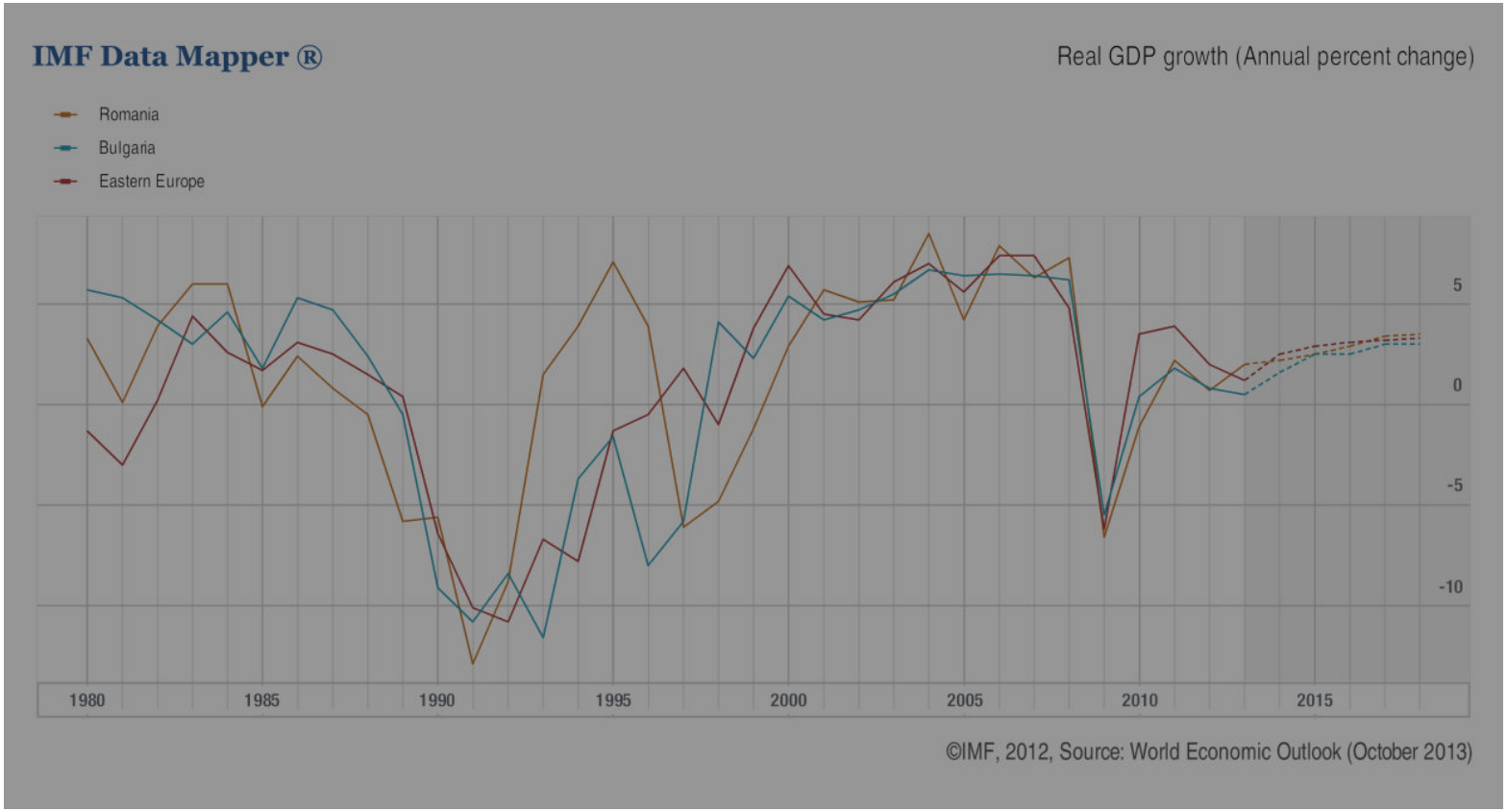
17.
Es ist möglich, dass die bereits herunter geladenen Kartendaten an andere Gruppen verkauft werden, wobei im Internet solche speziellen Seiten eingerichtet wurden, oder sie werden direkt an andere, dafür zuständige Teilnehmer der Gruppe, weitergegeben.

18. und 19.
Das erhaltene Geld wird von den Verantwortlichen innerhalb der Gruppen verteilt.

20.
Die Skimming-Täter sind Personen die kriminell auch für andere Taten, wie Schutzgelderpressung, Drogenhandel und Prostitution in Erscheinung getreten sind.

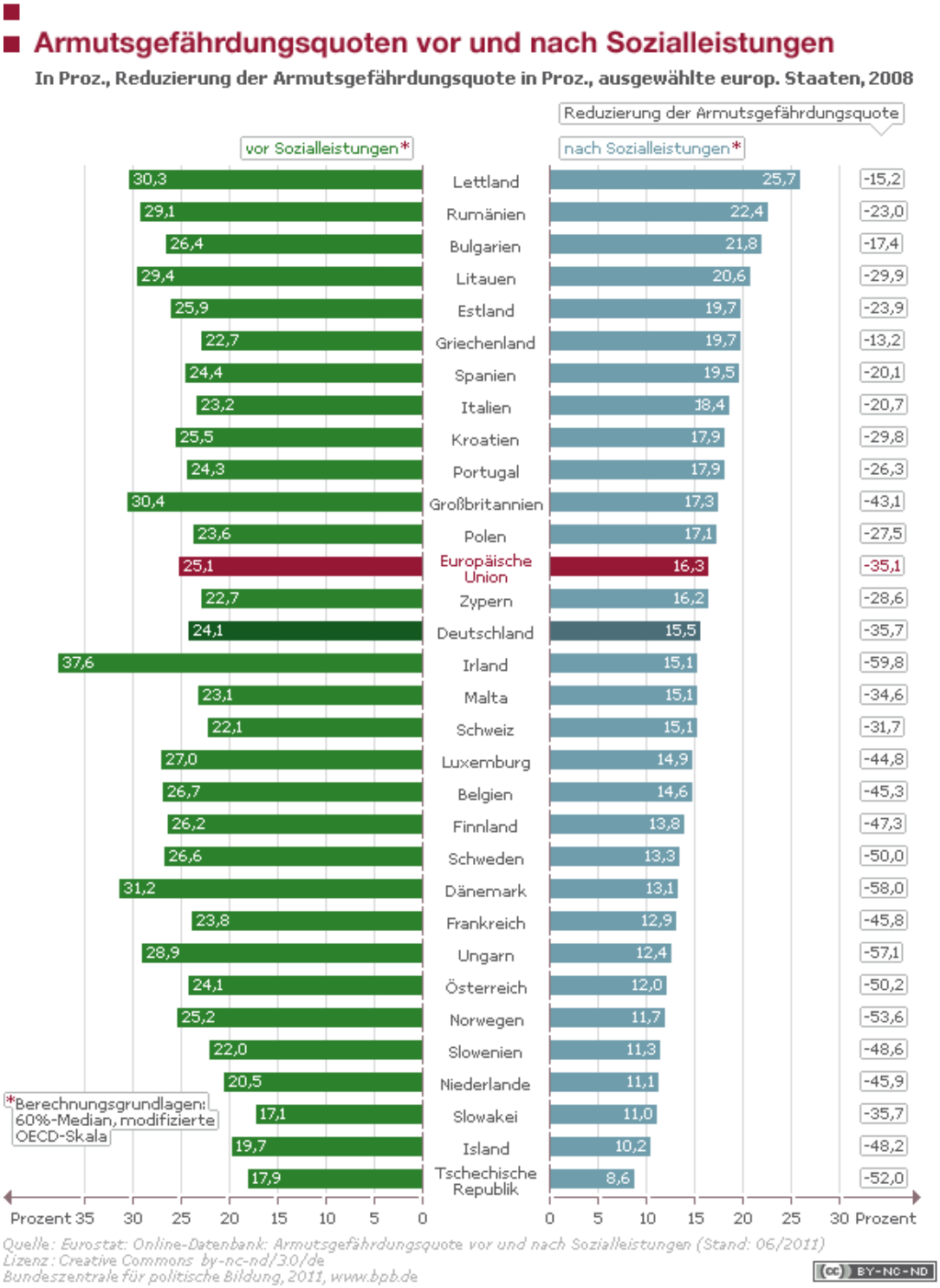
21.
In manchen Regionen des Landes sind besonders viele Personen die Skimming-Gerätschaften herstellen konzentriert, wie z.B. in Sofia, Plovdiv und Silistra. Aus diesen und andere Städten werden „Maultiere“ für Skimming rekrutiert.

Anlage 14: Entwicklung des Bruttoinlandsproduktes der Länder Bulgarien und Rumänien über den Zeitraum 1980 bis 2013



(International Monetary Fund 2013)

Anlage 15: Übersicht Armutsgefährdungsquote



(Bundeszentrale für politische Bildung 2011)

Erklärung über die selbstständige Abfassung der Masterarbeit

Hiermit versichere ich, dass ich die vorliegende Masterarbeit selbstständig gefertigt habe.

Alle wörtlichen Zitate wurden durch Anführungszeichen und Quellenverweise kenntlich gemacht.

Für die Erstellung der Arbeit wurden keine anderen Hilfsmittel benutzt, als die im Literaturverzeichnis angegebenen.

Frankfurt am Main, im Februar 2014 Anne Katharina Wonsack