Sozio-technische Aspekte von Finanz- und Cyberkriminalität

Ronny Merkel[1] · Jana Dittmann[1] · Stefan Reichmann[2]
Martin Griesbacher[2]

[1] Otto-von-Guericke Universität Magdeburg
Arbeitsgruppe Multimedia & Security
{ronny.merkel | jana.dittmann}@ovgu.de

[2] Karl-Franzens-Universität Graz
Institut für Soziologie
{stefan.reichmann | m.griesbacher}@uni-graz.at

Zusammenfassung

Straftaten im Bereich der Finanzkriminalität stellen eine andauernde Herausforderung für Aufklärungs- und Präventionsmaßnahmen dar. Besonders im Zuge der fortschreitenden Digitalisierung werden mehr und mehr auch digitale Mechanismen zu deren Bekämpfung eingesetzt, während menschliche und organisatorische Schwachstellen auch weiterhin ausgenutzt werden. Um die damit verbundenen Herausforderungen angemessen zu adressieren ist es notwendig, neben technischen Aspekten die unterschiedlichen Kriminalitätsformen auch aus einer psychologischen bzw. soziologischen Perspektive zu untersuchen. Im vorliegenden Beitrag werden Ergebnisse aus Interviews mit Straftätern aus dem Bereich der Finanzkriminalität sowie mit Experten aus dem Ermittlungsumfeld vorgestellt und diese vor dem Hintergrund des zunehmend an Bedeutung gewinnenden Bereichs der Cyberkriminalität diskutiert. Anhand von vier ausgewählten Modi Operandi von Straftaten mit Offline- und Online-Komponenten werden Anknüpfungspunkte für Schutzmechanismen aus sozio-technischer Sicht vorgeschlagen mit dem Ziel, Finanzkriminalität im Kontext von Cyberkriminalität als interdisziplinäres Problemfeld zur Verbesserung von Cybersicherheit verständlich zu machen.

1 Einleitung

Finanzkriminalität ist eine altbekannte Herausforderung, die jedoch im Zuge der Digitalisierung (auch) des Finanzsektors und den Verwerfungen und Chancen, die diese mit sich bringt, neuartige Fragestellungen und Probleme aufwirft [BuKr15b, Bäss15, EuPo15a, EuPo15b]. So bringt die sukzessive Einführung neuer Technologien auch stets neue (mitunter unentdeckte) Gefahrenpotenziale mit sich und erfordert die ständige Anpassung und Verbesserung der Sicherheitsinfrastrukturen und -maßnahmen. Zur umfassenden Verbesserung der Sicherheit, insbesondere im Zusammenhang mit neuen Informations- und Kommunikationstechnologien, braucht es auch ein umfassendes interdisziplinäres Verständnis typischer Verhaltensmuster von Tätern sowie Reaktions- und Umgangsweisen von Nutzern neuer Finanztechnologien. Um einen ganzheitlichen Schutz vor Auswirkungen und Folgen von Finanzkriminalität zu gewährleisten sind somit Strategien zur Erkennung, Aufklärung und Prävention von Vorfällen, zum Risiko- und Sicherheitsmanagement sowie deren kontinuierliche Verbesserung erforderlich, die

P. Schartner · A. Baumann (Hrsg.) · D•A•CH Security 2017 · syssec (2017) 24-37.

insbesondere auf dem Verständnis des relativ neuen Feldes der Cyberkriminalität aufbauen (siehe z.B. [UNDC13]).

Der vorliegende Beitrag beschäftigt sich in diesem Rahmen mit Finanzkriminalität im Kontext von Cyberkriminalität bzw. -sicherheit. Dabei werden die unterschiedlichen disziplinären Perspektiven der IT-Sicherheit, der Psychologie und der Soziologie betrachtet, mit dem Ziel, ausgewählte Aspekte der Finanz- und Computerkriminalität zu untersuchen und in ihrem Ablauf zu rekonstruieren. Es werden sowohl bereits bekannte als auch neuartige computer- bzw. internetbezogene Formen der Finanzkriminalität und die entsprechenden Handlungsmuster von Tätern diskutiert; letztere ergeben sich erst im Zuge der Digitalisierung von Finanzdienstleistungen und -produkten. Die Untersuchung stützt sich dabei auf den jeweiligen disziplinären Kenntnisstand sowie auf qualitative Interviews mit 24 Experten aus dem Ermittlungsumfeld (Ermittler, Kriminaltechniker, IT- und Finanzdienstleister) sowie 38 verurteilten Straftätern, die im Rahmen von Projekten zur Bezahlbetrugsbekämpfung in Österreich und Deutschland stattgefunden haben.

Dieser Beitrag soll einerseits zu einem verbesserten Verständnis des diffusen Forschungsfeldes der Cyberkriminalität beitragen, indem ein tieferer Einblick in die Modi Operandi von Cyberkriminellen ermöglicht wird, andererseits (und damit verbunden) werden auch konkrete Anknüpfungspunkte für Präventions- und Gegenmaßnahmen identifiziert. Am Beispiel der Finanzkriminalität zeigt sich zudem deutlich, dass im Zuge der Digitalisierung gänzlich neue Handlungsfelder, Angriffsmethoden und -ziele für Kriminalität ermöglicht werden und konkrete kriminelle Aktivitäten sich aus einem komplexen Set unterschiedlicher (teils konventioneller und teils computerbezogener) Komponenten zusammensetzen.

2 Finanzstraftaten im Kontext von Cyberkriminalität

Der vorliegende Beitrag untersucht verschiedene Formen von Finanzstraftaten im Kontext der Cyberkriminalität. Der Begriff der Finanzkriminalität ist dabei international nicht eindeutig definiert. Finanzkriminalität wird durch den internationalen Währungsfonds in einem weiten Sinne als jede Form gewaltloser Kriminalität verstanden, welche zu einem finanziellen Verlust führt [IMF01]. Dabei können sowohl Individuen und Firmen als auch Nationen von Finanzkriminalität betroffen sein [InPo17]. Finanzinstitutionen können beispielsweise als Opfer, Täter oder Tatmittel in Finanzkriminalität involviert sein [IMF01]. Oftmals werden Finanzdelikte dabei in Form organisierter Kriminalität durchgeführt [InPo17]. Delikte der Finanzkriminalität umfassen verschiedene Arten von Betrug (z.B. Falschdarstellung von Finanzdaten, Scheck- und Kreditkartenbetrug, Wertpapierbetrug, Versicherungsbetrug, Social-Engineering-Betrug), Unterschlagung, Bestechung, Erpressung, Geldwäsche, Fälschung von Zahlungsmitteln, Identitätsdiebstahl (in Kombination mit z.B. Betrug), Wucher, Finanzierung von Terrorismus und Wirtschaftskriminalität (z.B. Schneeballsysteme, Wertpapierbetrug) [FiLa17, InPo17, IMF01]. Dabei scheint der Finanzkriminalität besonders als Vortat zur Ermöglichung weiterer Straftaten eine zunehmend wichtigere Rolle zuzukommen [IMF01], weshalb sie an zentraler Stelle im Gesamtgefüge krimineller Aktivitäten steht. Sie kann wegen der teilweise bedeutenden Höhe entwendeter Geldsummen neben Individuen das gesamte ökonomische und soziale System beeinflussen und ist oftmals von internationaler Natur [InPo17].

„Cyberkriminalität“ bezeichnet nach der Budapester Konvention [EuKo01] jede kriminelle Handlung, die über Informationsnetzwerke und -infrastruktur abgewickelt wird und sowohl virtuelle als auch reale Räume zum Ziel hat. Es können verschiedene Bereiche cyberkrimineller

Handlungen unterschieden werden (siehe [Wall02, LKAB14, Yar06, ACB+16]): Cyber-Trespassing; Cyber-Theft [BGA+13]; Cyber-Pornographie und Cyber-Grooming; Rauschgifthandel und Waffenhandel; Verstöße gegen das Urheberrecht; Cyber-Violence (z.B. Cyberstalking etc.; vgl. [Yar06]). Auch andere, vor der Verbreitung des Internets bekannte Straftaten wie Beleidigung, Verleumdung, üble Nachrede, Volksverhetzung, Verletzung des höchstpersönlichen Lebensbereichs und Androhung von Straftaten sind hier relevant [EiPo14]. In dieser Aufzählung sollte bereits deutlich werden, dass Finanzkriminalität zwar nur einen Teil, aber doch verschiedene Arten von cyberkriminellen Aktivitäten umfasst, was auch die Ausführungen in den Abschnitten 3 und 4 zeigen werden. [UNDC13] unterscheidet 14 verschiedene Formen von Cyberkriminalität, wobei für die Finanzkriminalität folgende primär relevant sind: *illegal access to a computer system*; *illegal access, interception or acquisition of computer data*; *illegal data interference or system interference*; *computer-related fraud or forgery*. Sekundär relevant sind: *production, distribution of computer misuse tools*; *breach of privacy or data protection measures*; *sending or controlling sending of spam*; *computer-related acts in support of terrorism offences*. Der weltweite Anstieg cyberkrimineller Aktivitäten seit den 2000er Jahren wird v.a. auf die Verfügbarkeit entsprechender Technologien zurückgeführt [BGA+13]. Die Einführung neuer technischer Standards (z.B. Soziale Netzwerke, Smart Devices, Big Data) hat dabei Auswirkungen auf die Art der Kriminalität und ihre Bekämpfung [ACB+16]. Computer- bzw. internetbezogene Kriminalität ist durch mindestens einen der folgenden drei Aspekte charakterisiert [Wall02, ACB+16]:

1. Virtuelle Kommunikation und virtuelle Angebote unterstützten bzw. verschärfen bereits existierende Kriminalität (im Finanzbereich z.B. Betrug in Form von Online-Kreditbetrug oder Card-not-present-Betrug / Bestellbetrug, Identitätsdiebstahl mit dem Ziel von Betrug, Diebstahl von Zahlungskartendaten über Schadsoftware mittels RAM-Scraping).
2. Das Internet schafft ein neues transnationales Milieu für kriminelle Aktivitäten (im Finanzbereich z.B. durch Ermöglichung des Handels gestohlener Kreditkartendaten im Darknet, vereinfachte Beschaffung von Fälschungswerkzeugen wie Kartendubletten, Koordination international verteilter Straftaten wie beispielsweise beim Skimming in Land A und zugehöriger Bargeldabhebung mit gefälschten Kreditkarten in Land B).
3. Die durch das Internet möglich gewordene Entgrenzung von Raum und Zeit bringt gänzlich neue Typen von Kriminalität hervor (im Finanzbereich z.B. Relay-Angriffe auf kontaktlose Bezahlsysteme).

Durch neue Informations- und Kommunikationstechnologien ergeben sich daher drei (sich teilweise ergänzende) Funktionen für kriminelle Aktivitäten: 1. neue, zum Teil verstärkte Angriffsvektoren auf konventionelle Ziele (Technologie als erleichternde Instanz), 2. intensivierte und internationalisierte kriminelle Kooperation (organisierte Kriminalität) und 3. Ermöglichung neuer Angriffsziele. Dabei tritt Cyberkriminalität heute oftmals als industrialisierter Großzweig organisierter Kriminalität auf [BGA+13, Clou10]. Das Internet potenziert die Vernetzungsmöglichkeiten bereits bestehender krimineller Strukturen und schafft neue Wirkungsbereiche und Innovationspotentiale krimineller Aktivitäten [ACB+16].

Daneben wird das Internet auch von extremistischen Gruppierungen genutzt, da es zunehmend Teil der kritischen (nationalen und internationalen) Infrastruktur ist [Clou10]. Hier ergeben sich neben monetären auch politische, religiöse und ideologische Motivlagen, welche wiederum auch für Finanzkriminalität charakteristische Aktivitäten umfassen kann (z.B., wenn es darum geht, die Infrastruktur anzugreifen). Es gibt nicht immer einen klaren Zusammenhang zwischen

Tathergang und Motivlage; eine Tat, die auf den ersten Blick der Finanzkriminalität zugeschlagen wird, mag sich bei näherer Betrachtung als politisch motiviert herausstellen – und umgekehrt, wie beispielsweise beim sogenannten „BVB Anschlag“, bei dem ein Bombenanschlag mit Blick auf die Folgen am Aktienmarkt ausgeübt wurde.

Ob Cyberkriminalität als neuartige Form von Kriminalität aufzufassen ist bzw. inwieweit hierbei von einer Kontinuität zu herkömmlichen Formen auszugehen ist, ist vielfach umstritten [Yar06, Grab01]. Für [Will02] ist Cyberkriminalität lediglich eine Verlängerung „realer“ Kriminalität, die sich an den Möglichkeiten orientiert, die das Internet so oder so bietet (vgl. auch [Yar06] sowie [Grab01]). Allerdings bietet das Internet auch neue Möglichkeiten, die eigene Identität zu verschleiern oder im Extremfall neu zu schaffen [Will02], wobei es gleichzeitig zunehmend einfacher wird, vermeintlich anonyme Nutzer des Internet schlicht anhand von deren Suchverhalten zu identifizieren [Carr08].

[BGA+13] verweist darauf, dass die Tragweite von Cyberkriminalität vor allem darauf beruht, nationale und länderübergreifende Unterschiede in der Verbrechensaufklärung und -bekämpfung auszunutzen. [Clou10] gibt hier zu bedenken, dass viele Handlungen, die zunächst als cyberkriminell aufgefasst würden, bei näherer Betrachtung bloß den Charakter von Kommunikation haben, während die im eigentlichen Sinne kriminelle Handlung offline stattfindet. Der angerichtete Schaden hat in den meisten Fällen eine physische Komponente. Dies gilt auch für Finanzkriminalität dahingehen, weil es zur illegalen Aneignung der Verfügungsgewalt über Geld kommt. Im Nachfolgenden wird deutlich werden, wie neue Formen der Finanzkriminalität im Kontext von Cyberkriminalität verschiedenste sowohl computer- bzw. internetbezogene, als auch konventionelle Typen krimineller Handlungen umfassen.

3 Finanzkriminalität: Täter- und Expertensicht

Im Folgenden werden die Ergebnisse der Täter- und Expertenbefragungen hinsichtlich der Tatmotive, Modi Operandi sowie Geld-, Daten und Wissensflüsse zusammengefasst. Befragt wurden dabei 38 verurteilte Straftäter aus dem Bereich der Finanzkriminalität aus unterschiedlichen Jugendvollzugsanstalten der deutschen Bundesländer Bayern, Berlin, Niedersachsen, Sachsen und Sachsen-Anhalt sowie 24 deutsche und österreichische Experten aus dem Ermittlungsumfeld. Angesichts der international dünnen Datenlage können diese Einsichten dazu dienen, hier eine Forschungslücke in der Frage des Zusammenspiels von verschiedenen konventionellen und computerbezogenen kriminellen Aktivitäten zu schließen.

Motivlagen befragter Täter: Die Motive der Befragten Straftäter lassen sich mehrheitlich unter dem Gesichtspunkt der Bereicherung zusammenfassen. Die Lust an der persönlichen Bereicherung spielt dabei ebenso eine Rolle wie die Bestreitung von alltäglichen Ausgaben oder die Finanzierung von Süchten (Spiel- und Partysucht, Drogen, etc.). Die Erhaltung eines durch beruflichen Erfolg oder frühere Straftaten erlangten hohen Lebensstandards stellt ebenfalls ein maßgebliches Motiv für Straftaten dar. Dabei variiert die ursprüngliche Einkommenslage der Täter zwischen dem Bezug von Sozialhilfe und einem monatlichen Nettoeinkommen von bis zu 5000 €. In einigen Fällen ist schlicht Neugierde am Ausprobieren und Ausnutzen von Sicherheitslücken oder Abenteuerlust ausschlaggebend. Altruistische Motive wie beispielsweise die Begleichung von Gesundheitsausgaben für Angehörige und Freunde kommen vor, wenn auch eher selten.

Modus Operandi und Anpassungen: Der Einstieg ins kriminelle Milieu verdankt sich meist dem Ausprobieren einer Idee; diese wird oft von Freunden, Bekannten oder Verwandten angeregt. Nach erfolgreicher Tatausführung sowie dem Ausbleiben der Täterentdeckung und Sanktionierung besteht eine hohe Attraktivität der Tatwiederholung. Dabei sind einmal etablierte Modi Operandi oftmals stabil und werden nur in zweierlei Situationen aktualisiert: Zum einen durch Bekanntwerden neuer Informationen, welche die Tatausführung deutlich verbessern, zum andern durch die Einführung verbesserter Sicherheitsmechanismen seitens der Opfer, welche eine Adaption des Modus Operandi erforderlich machen. Beispiele für derartige Adaptionen sind die Anstellung zusätzlicher Täter bei Expansion (e.g. Läufer, Fahrer), die Einführung zusätzlicher Mechanismen zum Schutz vor Entdeckung oder Erhöhung des Gewinns sowie Mechanismen zur Umgehung eingeführter Schutzmaßnahmen.

Rückführung von Beute in den Geldkreislauf: Erbeutetes Geld wird schnellstmöglich in Bargeld umgewandelt, da dieses sich deutlich problemloser waschen, aufteilen und verstecken lässt, während Geldbewegungen von Giralgeld deutlich leichter von Aufklärungsbehörden nachvollzogen werden können. Neben der Verteilung und Reinvestierung des erhaltenen Bargelds wird dieses oftmals gewaschen, d.h. über festgelegte Wege in den legalen Geldkreislauf eingespeist, sodass dessen (scheinbar) legale Herkunft auf Anfrage nachgewiesen werden kann. Formen der Geldwäsche beinhalten dabei die Einzahlung, das Glücksspiel und spätere Auszahlung in Casinos, der Barkauf von Häusern, Autos und Waren, der Kauf und die darauffolgende Rückgabe von Waren, der Versicherungsbetrug mittels Zerstörung gekaufter Waren (z.B. absichtliche Herbeiführung von Unfällen gekaufter Autos) sowie die heimliche Vergrößerung der Erbmasse kürzlich verstorbener Angehöriger (z.B. Versteck von Bargeld im Haus von Verstorbenen, welches im Anschluss gefunden und geerbt wird). Neben der Rückführung von Beute in den legalen Geldkreislauf wird Bargeld oftmals versteckt (z.B. in Wohnungen und Schließfächern) sowie in den Besitz Unbeteiligter überführt, von welchen das Geld im Fall der Täterentdeckung nur schwer wieder eingezogen werden kann. So wurden Schenkungen von Bargeld und Häusern an vertrauenswürdige Verwandte und Freunde vorgenommen, welche die erworbenen Werte dann verwaltet, bewohnt, ins Ausland verbracht oder reinvestiert haben. Auch Einzahlungen in gemeinschaftlich genutzte Fonds kommen vor. Im Nachhinein können diese Einzahlungen meist nicht mehr dem Täter zugeordnet und somit nicht eingezogen werden.

Neben der Reinvestierung, Wäsche und dem Versteck erbeuteten Geldes wird dies auf vielfältige Art und Weise ausgegeben. Dabei werden von den Tätern Glücksspiel, Drogen, Partys und hohe Lebensstandards als Hauptausgabezwecke genannt. Autos, Immobilien und andere Luxusgüter spielen hier ebenfalls eine sehr große Rolle. Einmal erworbenes Bargeld wird wegen der Nachvollziehbarkeit digitaler Finanzströme nur in sehr seltenen Fällen zurück in Giralgeld überführt, in wenigen Fällen wurde die Nutzung von versteckten Konten im Ausland berichtet. Bitcoins scheinen hier hauptsächlich für Straftaten von Belang, welche zu großen Teilen im Cyberraum stattfinden. Sie kommen bei Straftaten mit erheblichen Offline-Komponenten bisher nur selten zum Einsatz. Nach der Verhaftung eines Täters kann das erbeutete Geld nur selten aufgefunden bzw. zurückgewonnen werden. Erbeutete Identitätsdaten werden durch die Täter meist zur Erzielung von Gewinn (z.B. Kreditkartendaten) oder zur Identitätsverschleierung (z.B. personenbezogene Daten Dritter zur Erstellung von gefälschten Identitätsdokumenten oder Liefer- bzw. Postadressen) eingesetzt.

Erwerb von tatrelevantem Wissen: Tatrelevantes Wissen wird häufig über soziale Kontakte erworben, in besonders starkem Maße von Mithäftlingen aus früheren Gefängnisaufenthalten aber auch aus Milieukontakten und Freundschaften zu Experten, wie Firmen-Insidern, Rechtsanwälten, Bankern, etc. In einigen Fällen konnte tatrelevantes Wissen über Schulungen und

universitäre Ausbildung, das Internet sowie Fernsehdokumentationen erworben werden. Dieser Befund deutet darauf hin, dass speziell computergestützte Finanzdelikte oftmals nicht technische, sondern menschliche bzw. organisatorische Schwachstellen ausnutzen.

4 Finanz- und Cyberkriminalität: Modi Operandi

Im Rahmen des vorliegenden Beitrags werden auf Basis der in den Täter- und Experteninterviews gewonnenen Erkenntnisse sowie weiterführender Literatur vier Modi Operandi (MO) der Finanz- und Cyberkriminaliät beschrieben. Dabei stellen die ersten drei Modi (MO1 - MO3) aktuelle Vorgehensweisen Krimineller dar, während der vierte Modus (MO4) einen bisher noch akademisches, jedoch für eine Umsetzung in naher Zukunft sehr realistisches Vorgehen beschreibt. In den nachfolgenden Ausführungen soll dabei auch deutlich werden, wie Finanzkriminalität an unterschiedlichen Schnittstellen eines Modus Operandi in jeweils variierenden Ausmaß auch mit Cyberkriminalität verbunden ist bzw. sein kann.

4.1 Sprengung von Geldautomaten (MO1)

Die Sprengung von Geldautomaten zur Erbeutung von Bargeld hat besonders in den letzten Jahren stark zugenommen. Allein im Jahr 2015 wurden in Deutschland 157 Spreng-Angriffe auf Geldautomaten verzeichnet, während es im Jahr 2011 lediglich 38 Angriffe waren [BuKr15a]. Bei dieser Straftat handelt es sich zwar um einen klassischen Modus Operandi der Finanzkriminalität, welcher weitgehend ohne digitale Werkzeuge durchgeführt wird (Abbildung 1, das Wiederholungspotential ist in Form einer gestrichelten Linie verdeutlicht), der aber auch insbesondere bei der Abwicklung im Vor- und Nachfeld der Sprengung heute bereits Elemente transnationaler und organisierter Kriminalität aufweisen kann. Dabei spähen die Täter im Vorfeld abgelegene bzw. niedrigfrequentierte Automaten aus. Zur Tatausführung fahren sie mit einem Fluchtfahrzeug meist nachts am Automaten vor, führen ein explosives Gasgemisch z.B. durch den Geldausgabeschacht in den Tresor des Automaten ein und bringen dieses mit einem Zünder zur Explosion. Ziel ist dabei, durch den Explosionsdruck ein Öffnen der Tresortür derart zu erreichen, dass das Geld der Automatenkassette entnommen werden kann. Die Täter entfernen sich im Anschluss mit dem Fluchtfahrzeug, bei grenznahen Automaten oftmals auch über Landesgrenzen hinweg, was eine Verfolgung zusätzlich erschwert.

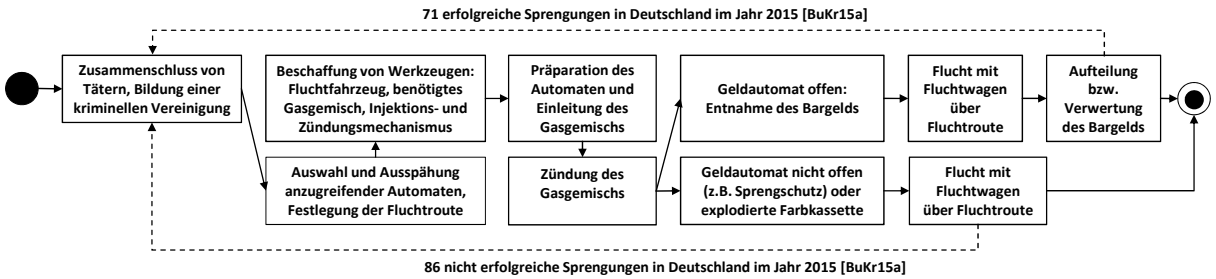

Abb. 1: Schematische Darstellung der Sprengung von Geldautomaten (MO1)

Die Sprengung von Geldautomaten birgt vielfältige Risiken für Täter und Unbeteiligte. Wird das Gasgemisch falsch gewählt, kann es zu Bränden und strukturellen Schäden an Gebäuden bzw. zu Verletzungen von Passanten und Anwohnern (aber auch der Täter selbst) kommen. Oftmals werden Geldautomaten weiterhin mit einem Sprengschutz versehen. In diesem Fall öffnet sich der Tresor trotz erfolgreicher Explosion nicht. Neben einem Sprengschutz werden in einigen Automaten auch Farbkartuschen verbaut, welche bei einer Explosion zerbersten, das

Geld in der Kassette einfärben und es somit unbrauchbar machen. Hierbei handelt es sich um eine Strategie, die auf der Ausnutzung sozialer Konventionen (in diesem Fall der Bargeldverwendung) fußt; derart gefärbte Geldscheine werden meist nicht als Zahlungsmittel akzeptiert bzw. erregen Verdacht, womit die Rückführung in den Geldkreislauf unterbunden wird.

Am Beispiel dieses Modus Operandi zeigen sich auch die Verdrängungseffekte von Kriminalität deutlich. Nachdem die Gesetzgeber einiger europäischer Länder eine Pflicht zur Installation von Farbkartuschen in Geldautomaten einführten, verlagerten sich die Sprengungen in Nachbarländer [Maus16]. So ist ein maßgeblicher Teil der grenznahen Sprengungen in der Bundesrepublik Deutschland auf niederländische Tätergruppen zurückzuführen. Die Flucht in ein Nachbarland bietet darüber hinaus weitere Vorteile, wie beispielsweise den Abbruch von Verfolgungen durch die Polizei an einigen Landesgrenzen.

4.2 Skimming am Geldautomaten (MO2)

Skimming bezeichnet das unbemerkte Auslesen von Bezahlkarten-Informationen Unbeteiligter. Diese können im Anschluss auf vielfältige Weise weitergenutzt werden, etwa zur Erstellung von Kartendubletten, zum Einkauf oder Abheben von Bargeld, zum Verkauf im Darknet sowie zum Erwerb von Waren im Internet (Card-not-present-Betrug). In einigen Fällen werden ebenso Offline-Zahlungen ohne die Vorlage einer Bezahlkarte allein auf Basis der Kartendaten akzeptiert. Dabei können Bezahldaten auf vielfältige Weise unbemerkt entwendet werden, wie beispielsweise durch die Anbringung eines Skimmers vor oder innerhalb eines Kartenleseschlitzes an Geldautomaten oder Bezahlterminals (Point-of-Sale, PoS). Mit Aufkommen des kontaktlosen Bezahlens ist ebenso das unbemerkte Auslesen von Kartendaten über Near Field Communication (NFC) möglich, welches als NFC-Skimming bezeichnet wird und den Auslesevorgang teilweise durch Handtaschen und Portemonnaies hindurch ermöglicht. Ein solcher Angriff wird dabei über das unbemerkte Anhalten von NFC-fähigen Lesegeräten (Smartphones, Kartenleser, PoS-Terminals) in größeren Menschenansammlungen auf öffentlichen Plätzen oder in Bussen und U-Bahnen realisiert.

Im Rahmen des vorliegenden Beitrags wird das klassische Skimming am Geldautomaten vorgestellt (MO2), bei dem die Bezahldaten eines Bankkunden durch Aufbringung eines Skimmers vor oder im Schlitz des Geldautomaten unbemerkt ausgelesen wird. Der gesamte Vorgang ist schematisch in Abbildung 2 dargestellt (das Wiederholungspotential ist in Form einer gestrichelten Linie verdeutlicht). Beim Skimming am Geldautomaten sind meist drei unterschiedliche Parteien beteiligt: Während sich der Manager um die Organisation der kriminellen Vereinigung sowie die Anwerbung von Läufern kümmert, erstellt der Techniker geldautomatenspezifische Hard- und Software, welche als Skimmer bezeichnet wird. Oftmals beinhaltet ein Skimmer auch eine zugehörige, separat versteckte Kamera, welche zur Erfassung der PIN beim Abhebevorgang dient (alternativ werden auch Aufsätze für Eingabetastaturen verwendet). Die eigentliche Installation und Deinstallation des Skimmers am Geldautomaten wird von Läufern ausgeführt, welche kurzfristig geschult und vergleichsweise gering entlohnt werden. Außer einem direkten Kontaktmann haben sie oft nur wenig Einblick in die Organisationsstruktur der Skimming-Vereinigung. Ein Skimmer wird im Regelfall wenige Stunden bis wenige Tage nach der Installation vom Läufer wieder entfernt, die erbeuteten Daten werden dem Techniker übergeben. Die Kartendaten werden im Anschluss in ein Zielland verbracht – welches magnetstreifenbasierte Geldautomat-Transaktionen erlaubt – und dort auf Kartendupletten geschrieben, welche zusammen mit der erbeuteten PIN zur Durchführung von Abhebungen an Geldautomaten genutzt werden. Für diese Abhebungen werden ebenfalls Läufer eingesetzt. Erbeutetes Geld

wird verteilt und verwertet. Der MO2 kann beliebig oft wiederholt werden. Im Jahr 2011 waren allein in Deutschland 1296 Skimming-Angriffe auf Geldautomaten zu verzeichnen [BuKr15a].

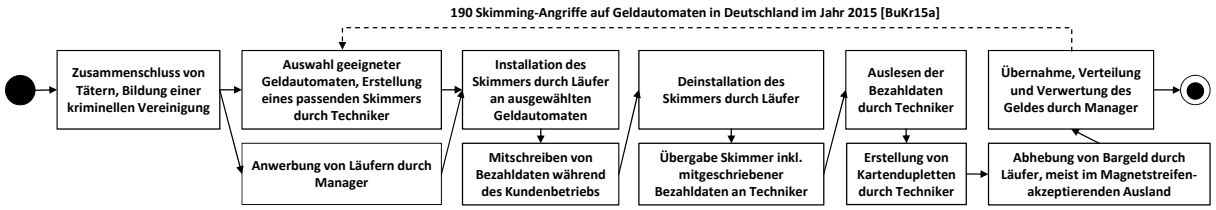

Abb. 2: Schematische Darstellung des Skimming am Geldautomaten (MO2)

Während die Tatausführung des Skimming-Vorgangs am Geldautomaten noch weitgehend offline durchgeführt wird, eröffnen sich bei der Weiterverwendung erbeuteter Bezahldaten besonders im Cyberbereich vielfältige Möglichkeiten. So können Kartendaten zum einen direkt digital verwertet werden, wie etwa durch den Verkauf im Darknet oder ihre Nutzung im Rahmen von Online-Einkäufen (Card-not-present-Betrug). Oftmals werden die Daten jedoch auch zur Erstellung gefälschter Kartendubletten verwendet, welche auf Basis von Magnetstreifentransaktionen Abhebungen oder Einkäufe im ausgewählten Zielländern ermöglichen. Hier bietet der Cyberraum indirekte Verwertungsmöglichkeiten sowie eine Entgrenzung von Kriminalität. So können Kartendaten in nur wenigen Sekunden in die Länder verbracht werden, in denen die entsprechenden Schwachstellen der Bezahl- und Abhebesysteme noch nicht geschlossen wurden.

Durch die zunehmende Verbreitung des EMV-Protokolls besonders in Europa sowie die Einführung des Geo-Blockings und die damit verbundene starke Reduktion zur illegalen Abhebung nutzbarer Geldautomaten ist auch die Anzahl der Skimming-Vorfälle deutlich zurückgegangen (190 Skimming-Angriffe auf Geldautomaten in Deutschland im Jahr 2015 [BuKr15a]). Jedoch weisen neben anderen Ländern besonders die USA noch einen hohen Anteil an Geldautomaten auf, welche Magnetstreifentransaktionen akzeptieren. Mit dem zu erwartenden Übergang der verbleibenden Länder zum EMV-Standard wird jedoch ein weiterer Rückgang von klassischen Skimming-Vorfällen an Geldautomaten einhergehen. Hier wäre es jedoch denkbar, dass neue Formen des Skimmings zukünftig entstehen, wie beispielsweise das unbemerkte Auslesen von Zahlungskarten über NFC-Funktionalität.

4.3 Online-Kreditbetrug (MO3)

Beim Online-Kreditkartenbetrug (Abbildung 3, Wiederholungspotential als gestrichelte Linie dargestellt) handelt es sich um eine klassische Straftat der Finanzkriminalität, welche jedoch teilweise auf computerbezogene Aktivitäten zurückgreift. Dabei werden mittels gefälschten Personalausweiskopien, Verdienstbescheinigungen und Kontoauszüge (unter anderem durch Ausnutzung einer Lücke im PostIdent-Verfahren [Scha15]) falsche Identitäten erstellt und mit diesen im Anschluss Online-Kredite beantragt. Das ausgezahlte Giralgeld wird auf Prepaid-Kreditkarten überwiesen, welche im Vorfeld (z.B. an Tankstellen) erworben wurden. Dies ermöglicht die unerkannte Abhebung und Verwertung der beantragten Kredite. Die Darstellung von MO3 basiert auf einem einzelnen Beispielfall, bei dem 10 Kredite erfolgreich beantragt und mehr als 25 Prepaid-Kreditkarten zur Auszahlung genutzt wurden. Während die Identifikation mittels PostIdent sowie die Auszahlung des Bargelds mehrheitlich offline erfolgen, findet die Beantragung der Kredite sowie die Aufteilung und Überweisung des erhaltenen Darle-

hens auf auszahlungsfähige Karten vollständig im Internet statt. Somit können die hier verfügbaren, digitalen Methoden zur anonymisierten, ferngesteuerten Kommunikation in Kombination mit einer gefälschten (einmal offline verifizierten) Identität genutzt werden.

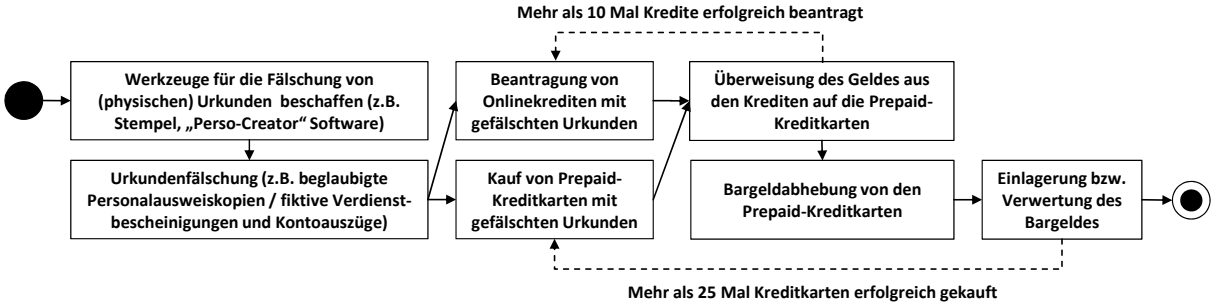

Abb. 3: Schematische Darstellung des Online-Kreditbetrugs (MO3)

An diesem Beispiel lässt sich weiterhin die These erhärten, wonach zusätzliche Sicherheitsmechanismen zur Abänderung eines Modus Operandi führen können. Dabei scheint es sich um eine Struktureigenschaft der Technikgenese und -entwicklung zu handeln, derart dass Technologien immer durch ihre Nutzer aufgenommen, interpretiert und adaptiert werden. Die sukzessive Erhöhung von technischen Sicherheitsmaßnahmen ist insofern illusorisch, als sich mit ihr auch die Bedingungen ändern, unter denen man Sicherheit herstellen will.

In dem hier untersuchten Fall wurden dabei die genutzten Prepaid-Karten durch starke Limitierungen seitens der herausgebenden Geldinstitute unbrauchbar. Das hat zu einer Verschiebung des Modus Operandi hin zur Beantragung falscher Bankkonten mitsamt gefälschter Kreditkarten geführt. Als Reaktion mussten mit den gefälschten Urkunden ebenfalls falsche Konten beantragt werden, dessen Karten an gefälschte Adressen mit Briefkastenzugriff gesendet wurden. Im Anschluss konnten so im vorgestellten Beispielfall mehr als 50 weitere Kredite beantragt und mittels der zu den Konten erworbenen Karten ausgezahlt werden.

4.4 Relay-Angriffe auf kontaktlose Bezahlsysteme (MO4)

Kontaktlose Bezahlfunktionen (über Near Field Communication, kurz NFC) erfreuen sich zunehmender Beliebtheit und Verbreitung. Dabei eröffnet die kontaktlose Übertragung von Bezahldaten neue Angriffsmöglichkeiten. Aufgrund der Neuheit dieses Verbrechenstypus liegen bislang noch keine Inhaftierungen (und damit auch keine Täterinterviews) vor. Allerdings weisen akademische Veröffentlichungen auf die technische Machbarkeit solcher Angriffe hin. Eine Form derartiger Angriffe stellt die sogenannte Relay-Attacke dar [BZP+14]. Dabei kooperieren zwei Täter miteinander, um eine künstliche Reichweitenvergrößerung von NFC-Bezahlkarten, die sich zumeist in den Taschen und Portemonnaies von Passanten befinden, zu erreichen. Bei dem Angriff wird mittels einer digitalen Informationsweiterleitung über das Internet ein Bezahlvorgang zwischen der Bezahlkarte des Opfers und einem entfernten Bezahlterminal durchgeführt (Abbildung 4, Wiederholungspotential als gestrichelte Linie dargestellt).

Beim Relay-Angriff werden zunächst zwei NFC-fähige, mobile Angriffsgeräte (z.B. Smartphones) benötigt, welche mit zugehöriger Relay-Software ausgestattet werden. Während sich ein Angreifer an öffentlichen Plätzen oder im Nahverkehr um eine möglichst starke Annäherung seines mobilen Angriffsgeräts an die in Hand- und Geldtaschen befindlichen kontaktlosen Bezahlkarten von Passanten bemüht, hält sich ein weiterer Angreifer in der Nähe eines Bezahlterminals auf. Hat der erste Angreifer eine Verbindung zu einer kontaktlosen Bezahlkarte etabliert,

leitet er die erhaltenen Bezahldaten über das mobile Angriffsgerät an den zweiten Angreifer weiter, welcher mit seinem Angriffsgerät einen kontaktlosen Bezahlvorgang an einem Terminal auslöst. Bei erfolgreicher Transaktion muss im Anschluss noch die gekaufte Ware in Bargeld überführt werden. Alternativ kann mittels einer eigenen Verkäufer-Bezahlinfrastruktur der Täter auch eine fingierte Transaktion ausgelöst werden, nach deren Abschluss das erbeutete Geld direkt im tätereigenen Verkäuferkonto zur Verfügung steht.

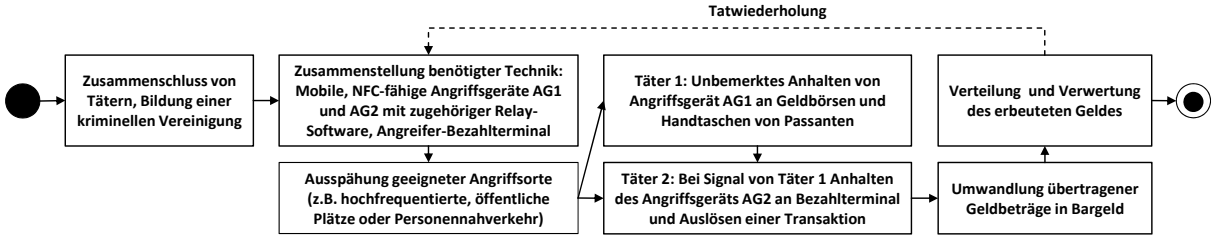

Abb. 4: Schematische Darstellung des Relay-Angriffs auf kontaktlose Bezahlsysteme (MO4)

NFC-basierte Relay-Angriffe sind in der Praxis bisher noch wenig verbreitet, stellen als vierter Modus Operandi jedoch eine fast vollständig digitalisierte Angriffsform und damit ein hohes Bedrohungspotential dar. Sieht man von der Auszahlung und Verwertung der Beute ab, so wird hier lediglich die Positionierung der beiden mobilen Angriffsgeräte in der Nähe der Opferkarte sowie des Bezahlterminals offline durchgeführt. Der Angriff könnte durch die Nutzung des Cyberraums noch weiter digitalisiert werden, um eine erhöhte Skalierbarkeit und damit verbundene Lukrativität zu erreichen. So können beispielsweise Smartphones mittels Schadsoftware direkt dazu genutzt werden, in Reichweite befindliche Bezahlkarten auszulesen (z.B. solche in der gleichen Handtasche oder Handyhülle), um diese für Relay-Attacken oder NFC-Skimming zu verwenden. Darüber hinaus kann Mobile-Wallet-Funktionalität auf dem befallenen Smartphone möglicherweise dazu genutzt werden, um auf dem Smartphone gespeicherte Bezahlinformationen zu missbrauchen. Besonders die massenhafte Verbreitung solchen Schadcodes führt zu einer deutlichen Erhöhung des Bedrohungspotenzials solcher internetbasierten Angriffe und erfordert ganzheitliche Schutzkonzepte, welche neben technischen Maßnahmen ebenso psychologische und gesellschaftliche Aspekte einbeziehen müssen.

5 Fazit: Verbesserung der Cybersicherheit

Die Auseinandersetzung mit den Modi Operandi zeigt auf, wie Finanzkriminalität im Kontext von Cyberkriminalität verschiedenste, teils computerbezogene Elemente aufweisen kann. Einerseits ermöglichen Informations- und Kommunikationstechnologien dabei die Stärkung (internationaler) krimineller Organisationsstrukturen sowie neue Angriffsmethoden und auch -ziele. Andererseits bleiben im Regelfall konventionelle physische Komponenten im Modus Operandi enthalten. So liegt allein der durch kriminelle Handlung entstandene Schaden auch bei den meisten Fällen von Cyberkriminalität offline, d.h. es kommt zu finanziellen oder (psycho-)physischen Nachteilen. Zwar sollte man daher, wie [Clou10] und andere anmerken, scharf zwischen „echter“ Cyberkriminalität, also solchen Formen von Kriminalität, die ohne Computer- und Internetbezug nicht existieren würden, und Formen, bei denen Computer(netzwerke) lediglich die Tatausführung erleichtern, unterscheiden. Doch bedeutet diese Unterscheidung keine prinzipielle Trennung von Finanz- und Cyberkriminalität, sondern sollte vordringlich zur Identifizierung von entsprechenden Schwachstellen in Finanzinfrastrukturen und -transaktionen und somit den entsprechenden Anknüpfungspunkten für Sicherheitsmaßnahmen dienen. Diese können einerseits auf die Verfolgung der Täter bzw. die Aufklärung von

Straftaten oder andererseits auf die Prävention bzw. Abschwächung der Tatbegehung und daraus entstehender Schäden abzielen.

Was bedeuten diese Erkenntnisse für die Sicherheit von mittlerweile auf Digitaltechniken beruhenden Finanzinfrastrukturen und -transaktionen bzw. für die *Cybersicherheit*? Bei der Begehung von Straftaten im Finanz- und Cyberkriminalitätsbereich werden nicht nur technische Schwachstellen ausgenutzt, sondern auch Organisationsstrukturen, kulturelle Faktoren (z.B. wenn Insiderwissen über Unternehmensstrukturen erworben wird) und Wissenslücken aufseiten des Personals. Teilweise geben auch Leichtgläubigkeit und mangelndes technisches Verständnis den Ausschlag. Im „Cyberspace" existiert – in Form des Darknets – außerdem ein relativ niederschwelliger Zugang zu Schadsoftware, Fälschungswerkzeugen etc. Wird solche Software genutzt, ist aufseiten der Kriminellen nicht einmal mehr besonderes technisches (i.e. Programmier-)Know-How erforderlich. Insgesamt lässt sich ableiten, dass neben technischen Sicherheitsmaßnahmen auch vermehrt Erkenntnisse der Psychologie und Soziologie relevant sind und Cybersicherheit somit vordringlich als *sozio-technisches* Problem verstanden werden muss, bei dem die künstliche Trennung zwischen technologie- und verhaltensbezogenen Sicherheitsmaßnahmen aufgebrochen wird. Das betrifft die Sensibilisierung von Privatpersonen und Unternehmen für einen fachgerechten Umgang mit sensiblen Daten und ein Gebrauchswissen über technische Maßnahmen wie auch die Gestaltung und Anpassung technischer und organisatorischer Sicherheitsvorkehrungen. Die nachfolgenden Anknüpfungsfelder sollen im Weiteren den breiten Möglichkeitsraum für Sicherheitsmaßnahmen verdeutlichen.

Technische Maßnahmen: Da Finanzinfrastrukturen und -transaktionen immer stärker diversifiziert und dezentralisiert werden (neue, kontaktlose Bezahlfunktionen mittels Smartphones, Wearables oder Bezahlstickern neben unterschiedlichster Geldautomaten und Bezahlterminals), steht bei technischen Maßnahmen die Frage von zeitgerechten Updates und Schließungen von entdeckten Sicherheitslücken eine zentrale Rolle. Dabei ist auf eine korrekte Implementierung von Transaktionsprotokollen und deren Sicherheitsmechanismen zu achten, deren Abwesenheit viele Straftaten erst ermöglicht. Bei der Umsetzung technischer Sicherheitsmaßnahmen stellt jedoch die Nutzerfreundlichkeit eine große Herausforderung dar, da sie Anforderungen an die Sicherheit oftmals gegenübersteht. Jedoch muss nicht in jedem Fall eine Sicherheitsmaßnahme auch einen Verlust an Nutzerfreundlichkeit bedeuten. So kann möglicherweise die elektronische Authentifizierung mittels eID den Prozess des Identitätsnachweises deutlich verkürzen, gleichzeitig jedoch die im MO3 ausgenutzte Schwachstelle schließen.

Schnittstellenbasierte Maßnahmen: Trotz einer hohen Bandbreite unterschiedlicher Straftaten der Finanz- und Cyberkriminalität ergeben sich einige typische Schnittstellen, welche von unterschiedlichen Tätern gleichermaßen genutzt werden. Solche Schnittstellen bilden z.B. die Geldkonvertierungsvorgänge, wie etwa die Umwandlung von digitaler Beute in Bargeld, aber auch die Wiedereinspeisung erbeuteten Geldes in den legalen Geldkreislauf (Geldwäsche). Sie bieten möglicherweise Angriffspunkte, um unterschiedliche Straftaten zu entdecken. Konkrete Maßnahmen müssen hier jedoch schnittstellenspezifisch angewendet werden (z.B. Herkunftsnachweis des Geldes bei größeren Barkäufen).

Vertrauens- und Akzeptanzdynamiken: Das Vertrauen der Kunden in digitale Infrastruktur ist ebenso aktiv herzustellen und zu fördern, etwa durch regelmäßige, sichtbare Updates und die Möglichkeit einer persönlichen Kontaktaufnahme. Insbesondere komplexe Sicherheitsvorkehrungen müssen auf die Akzeptanz der Nutzer bauen; das gilt sowohl für Offline- als auch Online-Maßnahmen. Dabei sollte das Vertrauen des Anwenders hergestellt werden, z.B. indem Sicherheitsmechanismen bereits im Designprozess berücksichtig und in ein Produkt vor seinem

Rollout eingebracht werden (Security by Design). Dies kann mit teilweise sehr einfachen Mitteln erreicht werden, wie beispielsweise der Nutzung eines Opt-in- anstelle eines Opt-out-Verfahrens (oder gar dem Ausrollen eines Produkts ohne vorherige Befragung des Nutzers) welches die potentiell als fehlend wahrgenommene Wahlfreiheit des Anwenders abmildern und eine höhere Sicherheitswahrnehmung hervorrufen kann. Vertrauens- und Akzeptanzdynamiken betreffen heute auch besonders die Nutzung personenbezogener Daten. Wo diese nicht vermieden werden kann (wie dies bei Finanzinfrastrukturen und -transaktionen in der Regel der Fall ist), sollte sie möglichst transparent nach dem Erforderlichkeitsprinzip gestaltet werden.

Motivlage der Täter: Hier kann eine Anreizverringerung auf technischer Ebene erfolgen (z.B. durch Verringerung der Erfolgsaussichten durch zusätzliche technische Schutzmechanismen), auf psychologischer (z.B. durch Optimierung von Sanktionierungsmaßnahmen) sowie gesellschaftlicher Ebene (z.B. durch Maßnahmen zur Sensibilisierung der Öffentlichkeit bezüglich Risiken und Gefahren neuer Informations- und Kommunikationstechnologien, insbesondere auch bezüglich Unterschieden in der medialen Wahrnehmung von Cyberkriminalität und tatsächlichen Risiken). Möglicherweise stellt auch die in sehr vielen Fällen beobachtete Wissensweitergabe innerhalb des Strafvollzugs einen potentiellen Anknüpfungspunkt dar, wobei sich die Schaffung angemessener Anreize zur Verhinderung eines solches Austausches innerhalb der Vollzugsanstalten jedoch als herausfordernd ergeben könnte.

Legistische Maßnahmen: Sicherheitsmaßnahmen haben meist Verdrängungseffekte zur Folge, wie beispielsweise die Verlagerung des Kreditkartenbetrugs in Länder mit magnetstreifenakzeptierenden Geldautomaten sowie die Verlagerung der Geldautomaensprengungen aus den Niederlanden nach Deutschland. Bei Online-Kriminalität sind solche Effekte jedoch schwierig nachzuweisen, da diese ohnehin meist länderübergreifend organisiert ist [Clou10, Wall02]. Abhilfe könnte hier eine bessere länderübergreifende Gesetzgebung schaffen, um hier zumindest legistische Lücken zu schließen. Legistische Maßnahmen funktionieren am besten dort, wo sie international abgestimmt und damit auch durchsetzbar sind (z.B. auf europäischer oder internationaler statt nationalstaatlicher Ebene), da es ansonsten zu den oben genannten Verdrängungseffekten kommt. Denkbar sind hier beispielsweise europaweit einheitliche Regelungen oder globale Übereinkünfte zur Schließung magnetstreifenbasierter und implementierungsbezogener Schwachstellen im Zahlungsverkehr. Dabei stellen legistische Maßnahmen auch ein Mittel dar, um von Finanzdienstleistern wegen Geringfügigkeit unadressierte Straftaten trotz ihrer geringen Kosten-Nutzen-Bilanz besser zu bekämpfen.

Kooperation internationaler Ermittlungsarbeit: Oftmals sind die Polizeibehörden bei Ermittlungen hinsichtlich grenzübergreifender Modi Operandi auf die Kooperation mit anderen Staaten angewiesen, z.B. im Rahmen eines Informations- und Know-How-Austauschs, abgestimmten Ermittlungen oder dem Nacheilen eines Täters in andere Länder. Eine reibungslose Zusammenarbeit bietet auch hier das Potential, Verdrängungseffekte und transnationale Kriminalität wirksam zu bekämpfen.

6 Zusammenfassung und Ausblick

Bei der Finanzkriminalität zeigt sich einmal mehr die Wucht nicht-intendierter Konsequenzen: Jede Gegenmaßnahme führt zumeist nicht zu einem Verschwinden der jeweiligen Tathandlungen, sondern entweder zur Adaptierung der Vorgehensweise oder zum Ausweichen in einen anderen Rechtsraum. Dies zeigt sich deutlich, wenn man internationale Daten zur Finanzkriminalität vergleicht, etwa am Beispiel der Verlagerung von Geldautomatensprengungen oder

Skimming infolge veränderter technischer Rahmenbedingungen. Die Verdrängungseffekte können aber nicht nur regionale Verschiebungen zur Folge haben, sondern auch die Suche nach neuen Angriffsmethoden und -zielen betreffen: Einerseits durch Rückverlagerung auf konventionelle Methoden, wenn computerbezogene Angriffe nicht mehr funktionieren; andererseits auf soziotechnische Schwachstellen bei neuen Bezahltechnologien.

Die Analyse von Finanzstraftaten im Kontext von Cyberkriminalität weist darauf hin, dass kontinuierlich mit neuartigen Angriffsmethoden und -zielen gerechnet werden muss, welche die Cybersicherheit gefährden, jedoch in der Regel auch neue Anknüpfungspunkte für Sicherheitsmaßnahmen beinhalten. Dabei kann Cybersicherheit nicht nur *ex negativo* als *Abwesenheit* von Cyberkriminalität verstanden werden. Ein erweiterter Begriff von Cybersicherheit schließt auch die Wahrnehmung von Risiken und damit die Vertrauens- und Akzeptanzdynamiken im Zusammenhang mit dem virtuellen Raum ein, die mit unterschiedlichen Akteursgruppen assoziiert werden. Dabei sind nicht nur Kriminelle zu nennen, sondern auch staatliche, wirtschaftliche oder politische Akteure, deren Handeln sich v.a. auf sensible Bereiche wie den Umgang mit personenbezogenen Daten im Allgemeinen oder Überwachung im Speziellen bezieht [Garl08]. Eine totale Kontrolle aller Risiken und unvorhergesehenen Konsequenzen von Kriminalität und Sicherheitsmaßnahmen erscheint dabei zwar illusorisch, aber nur die stetige Verbesserung von investigativen, verhindernden und abschwächenden Sicherheitsmaßnamen auf interdisziplinärer Basis kann hier eine Annäherung bringen.

Danksagung

Teile dieser Veröffentlichung entstanden aus dem Forschungsvorhaben „Organisierte Finanzdelikte – methodische Analysen von Geld-, Daten- und Know-How-Flüssen (INSPECT)“ mit dem Förderkennzeichen 13N13473 (gefördert vom Bundesministerium für Bildung und Forschung, BMBF) und dem Projekt „Bezahlbetrugsbekämpfung bei modernen, mobilen Methoden (3B3M)“ (finanziert im Sicherheitsforschungs-Förderprogramm KIRAS vom österreichischen Bundesministerium für Verkehr, Innovation und Technologie).

Literatur

[ACB+16] B. Akhgar, M. Choras, B. Brewster, F. Bosco, E. Vermeersch, V. Luda, D. Puchalski, D. Wells: Consolidated Taxonomy and Research Roadmap for Cybercrime and Cyberterrorism. In: B. Akhgar, B. Brewster (Hrsg.): Combatting Cybercrime and Cyberterrorism. Challenges, Trends and Priorities. Springer (2016), 295-321.

[Bäss15] J. Bässmann (BKA Deutschland): Täter im Bereich Cybercrime - Eine Literaturanalyse. Online: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/Forschungsergebnisse/2015TaeterImBereichCybercrime.html (02.03.2017).

[BGA+13] R. Broadhurst, P. Grabosky, M. Alazab, B. Bouhours, S. Chon, C. Da: Crime in Cyberspace: Offenders and the Role of Organized Crime Groups. Working Paper: Australian National University Cybercrime Observation Laboratory (2013).

[BuKr15a] BKA Deutschland: Bundeslagebild Angriffe auf Geldautomaten 2015. Online: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/AngriffeGeldautomaten/angriffeAufGeldautomaten_node.html (12.05.2017).

[BuKr15b] BKA Österreich: Cybercrime – Jahresbericht 2015. Online: http://www.bmi.gv.at/cms/BK/publikationen/Cybercrime.aspx (02.03.2017).

[BZP+14] J. van den Breekel, N. Zannone, E. Poll, J. de Ruiter, S. Hegt, T. Timmerman (K.P.M.G. Netherlands): A security evaluation and proof-of-concept relay attack on Dutch EMV contactless transactions. Doctoral dissertation, Master thesis, Technische Universiteit Eindhoven (2014).

[Carr08] N. Carr: The Big Switch. Rewiring the World, From Edison to Google. New York, London: W. W. Norton & Company (2008).

[Clou10] J. Clough: Principles of Cybercrime. Cambridge et al.: Cambridge University Press (2010).

[EiPo14] S. Eifler, D. Pollich: Empirische Forschung über Kriminalität. Methodologische und methodische Grundlagen. Wiesbaden: Springer (2014), XV 474.

[EuKo01] CoE: Conv. on Cybercrime. Online: www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (16.06.2017).

[EuPo15a] Europol: The Internet Organised Crime Threat Assessment (IOCTA) 2015. Online: https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015 (02.03.2017).

[EuPo15b] Europol: Exploring Tomorrow's Organized Crime. Online: https://www.europol.europa.eu/publications-documents/exploring-tomorrow%E2%80%99s-organised-crime (02.03.2017).

[FiLa17] FindLaw: Fraud and Financial Crimes. Online: http://criminal.findlaw.com/criminal-charges/fraud-financial-crimes.html (13.06.2017).

[Garl08] D. Garland: Kultur der Kontrolle. Verbrechensbekämpfung und soziale Ordnung in der Gegenwart. Frankfurt am Main: Campus (2008).

[Grab01] P. Grabosky: Virtual Criminality: Old Wine in New Bottles? In: Social and Legal Studies 10 (2), (2001), 243-249.

[IMF01] International Monetary Fund: Financial System Abuse, Financial Crime and Money Laundering - Background Paper. Online: https://www.imf.org/external/np/ml/2001/eng/021201.pdf (13.06.2017).

[InPo17] INTERPOL: Financial crime. Online: https://www.interpol.int/Crime-areas/Financial-crime/Financial-crime (13.06.2017).

[LKAB14] LKA Baden-Württemberg: Cybercrime / Digitale Spuren. Jahresbericht (2014).

[Maus16] J. Mausch: Tinte und Tresor: Banken rüsten nach Automatensprengungen auf. Online: https://www.noz.de/lokales/meppen/artikel/668089/tinte-und-tresor-banken-rusten-nach-automatensprengungen-auf (15.06.2017).

[Scha15] P. Schader: Sicherheitsmängel bei Postident: Eintrittskarte für den organisierten Betrug. Online: https://krautreporter.de/711--sicherheitsmangel-bei-postident-eintrittskarte-fur-den-organisierten-betrug (13.06.2017).

[UNDC13] United Nations Office on Drugs and Crime (Hrsg.): Comprehensive Study on Cybercrime. New York: United Nations (2013).

[Wall02] D. Wall: Cybercrimes and the internet. In: D. Wall (Hrsg.): Crime and the Internet. London, New York: Routledge (2002), 1-17.

[Will02] M. Williams: The language of cybercrime. In: D. Wall (Hrsg.): *Crime and the Internet*. London, New York: Routledge (2002), 152-166.

[Yar06] M. Yar: Cybercrime and Society. London u.a.: Sage (2006).