Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD

Bundesamt für Polizei fedpol
Bundeskriminalpolizei BKP
Abteilung Kriminalanalyse

National Risk Assessment (NRA):

Betrug und Phishing zwecks betrügerischen Missbrauchs einer Datenverarbeitungsanlage als Vortat zur Geldwäscherei

Bericht der interdepartementalen Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT)

Januar 2020

Inhaltsverzeichnis

Executive Summary

Mit der zunehmenden Digitalisierung der Gesellschaft nimmt weltweit die Bedeutung der Internetkriminalität Jahr für Jahr zu. Ein grosser Teil der im Internet verübten Straftaten sind Betrugsdelikte. Die betrügerisch erlangten Gelder werden anschliessend gewaschen, nicht selten mittels sogenannter Finanzagenten. Im Dezember 2019 konnten beispielsweise in einer von Europol unterstützten internationalen Grossaktion gegen Geldwäscherei über 3800 Finanzagenten identifiziert und 228 davon verhaftet werden.[1] Aber auch ausserhalb des digitalen Raums finden weiterhin Betrüge statt. Auch die Schweiz ist vom Phänomen betroffen. Betrug und sein digitales Pendant, der betrügerische Missbrauch einer Datenverarbeitungsanlage (Missbrauch einer DVA), machen seit Jahren einen grossen Teil der Verdachtsmeldungen an die Meldestelle für Geldwäscherei und Terrorismusfinanzierung (MROS) aus. Vor allem der Betrug war mit fast 40 Prozent aller Verdachtsmeldungen zwischen 2004 und 2014 die am häufigsten vermutete Vortat (Missbrauch einer DVA: 4%). Inzwischen stehen zwar Korruptionsdelikte an erster Stelle der Verdachtsmeldungen. Aber Betrug und, in geringerem Ausmass, der Missbrauch einer DVA, bleiben häufig vermutete Vortaten von Geldwäschereihandlungen. Aus diesen Gründen hat die Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT) entschieden, die Geldwäschereivortaten Betrug und Phishing zwecks betrügerischen Missbrauchs einer DVA in der Schweiz genauer zu erforschen.

Grundsätzlich stellt jeder erfolgreiche Betrug im strafrechtlichen Sinn und jeder erfolgreiche betrügerische Missbrauch einer DVA eine mögliche Vortat zur Geldwäscherei und somit eine potenzielle Geldwäschereigefahr dar. Vorausgesetzt wird lediglich, dass die Straftat nicht als geringfügiges Vermögensdelikt eingestuft wird. Statistiken und Opferbefragungen zeigen, dass diese beiden Betrugsdelikte in der Schweiz zwar weit verbreitet sind, aber nicht so häufig vorkommen wie andere Vermögensdelikte wie beispielsweise Diebstahl. Die aktuelle lückenhafte Faktenlage über den Umfang der Vortaten im Ausland mit anschliessenden Geldwäschereihandlungen in der Schweiz erlaubt es nicht, präzise Schlussfolgerungen ziehen zu können. Wie bei den Vortaten hierzulande dürfte auch in solchen Fällen die durchschnittliche Schadensumme verhältnismässig tief sein; in der Mehrheit der Fälle liegt sie im drei- bis vierstelligen Bereich. Letztlich bleiben viele Betrugsfälle beim Versuch und bilden somit keine Vortat zur Geldwäscherei. Aus diesen Gründen ist für die Schweiz von einer höchstens mittleren Geldwäschereigefährdung durch Betrug und betrügerischem Missbrauch einer DVA auszugehen.

Betrugsdelikte sind allerdings sehr vielfältig und unterscheiden sich betreffend Anzahl Opfer, Komplexität, Schadensumme oder Modus Operandi stark. Grundsätzlich finden zumeist Betrüge statt, die massenhaft und mit relativ wenig Aufwand durchgeführt werden können, im Durchschnitt aber auch weniger kriminelle Erträge pro Fall einbringen. Typische Beispiele dafür sind Betrüge beim Onlineshopping oder auf Immobilienplattformen, wo die Schadensumme pro Opfer meistens im zwei- oder dreistelligem Bereich liegt. Anderseits gibt es Betrugsphänomene, die zahlenmässig seltener gelingen dürften, die aber den Kriminellen hohe Erträge versprechen. Dafür müssen die Täter im Schnitt mehr Zeit investieren, wie beispielsweise bei falschen Hilfeleistungen oder falschen Überweisungsaufträgen. In solchen Betrugsfällen beträgt die fallbezogene Schadensumme regelmässig mehrere hunderttausend Franken. Insgesamt sind die Schadensummen beim Staat und bei Unternehmern durchschnittlich um einiges höher als bei privaten Personen. So werden in den meisten Fällen verhältnismässig tiefe Geldsummen gewaschen, typischerweise mithilfe von Finanzagenten. Geldwäschereihandlungen

[1] EUROPOL (2019): 228 arrests and over 3800 money mules identified in global action against money laundering. Medienmitteilung vom 04.12.2019. https://www.europol.europa.eu/newsroom/news/228-arrests-and-over-3800-money-mules-identified-in-global-action-against-money-laundering.

mit grösseren Summen kommen zwar vor, sind allerdings selten. Beispielsweise betrafen zwischen 2009 und 2018 weniger als 2% der Verdachtsmeldungen an MROS wegen Betrug Summen über 10 Millionen Franken.

Die grössten Verwundbarkeiten bilden der Einsatz von Finanzagenten und juristischen Personen mit Sitz im Ausland. Zudem ergeben sich aufgrund neuerer Informations- und Kommunikationstechnologien zahlreiche Möglichkeiten zur Internationalisierung der Vortaten und der damit verbundenen Geldwäscherei. Informationen über den Einsatz von Krypto-Assets zum Zwecke der Geldwäscherei nach Betrugsdelikten sind noch lückenhaft; solche Technologien stellen aber potenziell eine grosse Verwundbarkeit dar. Auch die Komplexität des Betrugstatbestands, das rechtzeitige Abschöpfen von Vermögenswerten oder der Nachweis der Vortat stellen je nach Konstellation eine Herausforderung für die Strafbehörden dar.

Die Folgen von Betrugsdelikten als Vortat zur Geldwäscherei sind schwierig abzuschätzen, scheinen sich aber, dank eines grundsätzlich wirksamen Abwehr- und Bekämpfungsdispositivs, nicht auf die Gesellschaft, den Finanzsektor oder Dienstleistungsbereiche als Ganzes auszuwirken. Zwar können die finanziellen Schäden für einzelne Opfer oder auch den Staat erheblich sein, die Möglichkeiten der Vermögensabschöpfung und Ersatzforderungen können diese Schäden jedoch teilweise mindern. Präventive Wirkung kann auch die Geldwäschereigesetzgebung entfalten, indem sie es ermöglicht, gewisse verdächtige Zahlungen zu stoppen.

Das Ausmass und die Wirkung von Geldwäschereihandlungen aus dem Betrug und dem Missbrauch einer DVA stellen in ihrer Gesamtheit bislang keine systemrelevante Gefahr für die Schweiz dar. Die Bedrohungslage betreffend Betrugsdelikte als Vortat zur Geldwäscherei hat sich somit in den letzten Jahren nicht wesentlich verändert. Wie diese sich in näherer Zukunft entwickeln wird, hängt wesentlich von der Entwicklung der Internetkriminalität ab. Die aktuelle Faktenlage ist allerdings noch zu dürftig, um eine genaue Prognose abgeben zu können. Dafür sind weitere wissenschaftlich durchgeführte Studien, insbesondere auf Betrugsdelikte fokussierte Opferbefragungen, einer unabhängigen Forschungsstelle (zum Beispiel Universitäten), nötig.

1 Einleitung

1.1 Hintergrund NRA-Gesamtbericht und Auftrag

Im Juni 2015 wurde der erste Bericht über die nationale Beurteilung der Geldwäscherei- und Terrorismusfinanzierungsrisiken in der Schweiz (NRA-Bericht) publiziert.[2] Der Bericht wurde von der Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT) erarbeitet. Diese wurde Ende 2013 vom Bundesrat gegründet und «hat die Aufgabe, die Massnahmen im Zusammenhang mit der Bekämpfung der Geldwäscherei und Terrorismusfinanzierung innerhalb der Bundesverwaltung zu koordinieren. In diesem Rahmen hat sie insbesondere für eine ständige Risikobeurteilung zu sorgen, mit dem Ziel, neue Geldwäscherei- und Terrorismusfinanzierungsbedrohungen zu erkennen und allfällige Massnahmen zu deren Eindämmung vorzuschlagen.»[3] Durch die Einsetzung der KGGT setzt die Schweiz die Empfehlungen 1 und 2 der *Groupe d'action financière* (GAFI) um, welche eine nationale Risikoanalyse (*national risk assessment* NRA), einen risikobasierten Ansatz sowie eine Behörde bzw. einen Mechanismus zur Koordination der nationalen Politik zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung verlangen.[4] Diese Risikoanalyse sieht ein fortdauerndes Identifizieren und Bewerten der Risiken im Bereich der Geldwäscherei und der Terrorismusfinanzierung vor («*identify and assess their ML/TF* [*Money Laundering*/*Terrorist Financing*] *risks on an 'ongoing basis'*»).[5]

Um die Gefährdung der Schweiz durch Geldwäscherei beurteilen zu können, wurden bei der Erstellung des NRA-Berichts unter anderem auch Informationen aus den Verdachtsmeldungen an die Meldestelle für Geldwäscherei (MROS) ausgewertet. Gemäss diesen war mit fast 40% aller Verdachtsmeldungen Betrug zwischen 2004 und 2014 die am häufigsten vermutete Vortat (betrügerischer Missbrauch einer Datenverarbeitungsanlage: 4%).[6] Seitdem sind allerdings – mit Ausnahme von 2016 – Korruptionsdelikte an erster Stelle. Betrugsdelikte bleiben aber weiterhin häufig gemeldete Vortaten. Aus diesem Grund hat die KGGT entschieden, die Geldwäschereivortaten Betrug und Phishing zwecks betrügerischen Missbrauchs einer Datenverarbeitungsanlage sowie konsekutive Geldwäschereihandlungen in der Schweiz genauer zu erforschen.

Gemäss diesem Auftrag gibt der vorliegende Analysebericht zunächst einen kurzen Überblick über die wichtigsten Akteure im Bereich Betrugsprävention und -bekämpfung. Im zweiten Kapitel werden die relevanten Straftatbestände behandelt und erste Abgrenzungsfragen geklärt. Die Gefährdung, die für die Schweiz aus den Betrugsdelikten als Vortat zur Geldwäscherei ausgeht, wird im Kapitel 3 analysiert. Das Kapitel 4 ist der Verwundbarkeit und den Herausforderungen gewidmet. Die Analyse der potenziellen Folgen sowie die zusammenfassende Risikobewertung werden schliesslich in Kapitel 5 vorgenommen.

1.2 Methodik

Der vorliegende Bericht stützt sich auf die Verdachtsmeldungsstatistik der MROS aus den letzten zehn Jahren (2009-2018)und auf die Auswertung von 69 Entscheiden von Gerichten

[2] KGGT (2015a): Bericht über die nationale Beurteilung der Geldwäscherei- und Terrorismusfinanzierungsrisiken in der Schweiz. https://www.fedpol.admin.ch/dam/data/fedpol/kriminalitaet/geldwaescherei/nra-berichte/nra-bericht-juni-2015-d.pdf.

[3] KGGT (2015b): Medienmitteilung zum Bericht über die nationale Beurteilung der Geldwäscherei- und Terrorismusfinanzierungsrisiken in der Schweiz. https://www.news.admin.ch/message/index.html?lang=de&msg-id=57750.

[4] Vgl. GAFI (2012): International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations. Aktualisiert im Juni 2019. https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.

[5] GAFI (2013): National Money Laundering and Terrorist Financing Risk Assessment. FATF Guidance, February 2013. www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf, S. 6.

[6] KGGT (2015a), op. cit., S. 35.

und Staatsanwaltschaften aus den Jahren 2015 bis 2018, die MROS zur Verfügung standen.[7] Ebenfalls wurde auf öffentlich zugängliche Quellen wie Kriminal- oder Strafurteilsstatistiken sowie Fachliteratur zurückgegriffen. Bei der Auswahl der Justizentscheide wurde vor allem auf die Vielfalt Wert gelegt. Die untersuchten Entscheide sind aber nicht repräsentativ für die Häufigkeit der jeweiligen Betrugsarten. Zusätzlich wurden Gespräche mit Vertretern der MROS sowie der Bundeskriminalpolizei (fedpol), der Schweizerischen Kriminalprävention (SKP), der Bundesanwaltschaft (BA) und einer kantonalen Staatsanwaltschaft geführt.

Hauptteil des Berichtes ist die Bewertung des Geldwäschereirisikos. Die GAFI verwendet für die Bewertung der Geldwäscherei- und Terrorismusfinanzierungsrisiken einen Risikobegriff, der sich aus den drei Faktoren Gefährdung, Verwundbarkeit und Folgen (*threat*, *vulnerability* und *consequence*) zusammensetzt.[8]

Die Gefährdungen (*threats*) sind definiert als die Wahrscheinlichkeit, dass eine Person oder eine Gruppe von Personen Geldwäschereihandlungen vornimmt. Die Bedrohungsbeurteilung (*threat assessment*) hingegen ermittelt die Bedeutung der Gefährdung, indem sowohl ihr Ausmass (quantitatives Element) als auch ihre Merkmale (qualitatives Element) gemessen werden. Dabei muss zwischen potenziellen und reellen Gefährdungen unterschieden werden. Die potenzielle Gefährdung (oder abstrakte Gefährdung) bezeichnet die Wahrscheinlichkeit, dass eine Bedrohung angesichts gewisser struktureller und kontextueller Elemente eintreffen könnte. Die reelle Gefährdung (oder konkrete Gefährdung) ist die Gesamtheit aller Gefährdungen, die effektiv eingetroffen sind und die grundsätzlich gemessen werden können.

Die Verwundbarkeiten (*vulnerabilities*) sind die Gesamtheit aller (strukturellen und institutionellen) Faktoren, die das Begehen eines Verbrechens in den Augen der Person oder der Gruppe von Personen, die Geld waschen wollen, attraktiv machen. Die Wahrscheinlichkeit, dass sich ein Risiko verwirklicht, ist umso höher, je mehr Verwundbarkeiten existieren. Die allgemeinen Verwundbarkeiten hängen mit den strukturellen Merkmalen eines Landes und seines Finanzplatzes zusammen. Die spezifischen Verwundbarkeiten sind mit den Praktiken und Instrumenten verbunden, die in einem bestimmten Tätigkeitsbereich verwendet werden. Eine letzte Kategorie ist jene der Verwundbarkeiten im Zusammenhang mit dem institutionellen Dispositiv (Regulierung und Aufsicht) im Kampf gegen die Geldwäscherei.

Als Folgen (*consequences*) versteht man die Wirkung oder der Schaden, der aufgrund der Geldwäscherei entstehen kann.

1.3 Überblick Prävention und Bekämpfung

In der Schweiz widmen sich verschiedene Stellen der Prävention und der Bekämpfung von Betrug im umgangssprachlichen Sinn[9]. Im Folgenden werden die wichtigsten Akteure und ihr jeweiliger Auftrag kurz umschrieben.

Nationale Cyber-Kompetenzzentrum (NC3) bei fedpol
Das Bundesamt für Polizei fedpol ist, unter anderem, die schweizerische Zentralstelle im Bereich der Internetkriminalität. Somit obliegen fedpol in der Zusammenarbeit mit den Kantonen und innerhalb von NEDIK (siehe unten) Zentralstellenaufgaben. So unterstützt fedpol zum Beispiel die Kantone mit IT-Forensik-Leistungen, in der Fallkoordination und Triage, mit (hoch-)spezialisierten Fachkompetenzen oder Infrastruktur. Das 2017 bei fedpol gebildete nationale Cyber-Kompetenzzentrum (NC3) fasst sämtliche cyber-relevanten Kompetenzen aus den fedpol-Bereichen Ermittlungen, Ermittlungsunterstützung und Zentralstellenaufgaben zusammen.

[7] 1 Nichteintretensentscheid, 42 Einstellungsverfügungen, 2 Freisprüche, 10 Strafbefehle und 14 Schuldsprüche. Zehn Verfahren wurden durch die Bundesanwaltschaft und die restlichen durch kantonale Strafverfolgungsbehörden geführt. Mindestens 43 dieser Verfahren wurden durch eine Verdachtsmeldung an MROS initiiert.
[8] GAFI (2013), op. cit., S. 7–8.
[9] Betrug im umgangssprachlichen Sinn geht über den Tatbestand des Art. 146 StGB hinaus. Vgl. dazu Kapitel 2 des vorliegenden Berichts.

Meldestelle für Geldwäscherei MROS bei fedpol[10]
Der Meldestelle für Geldwäscherei (MROS) im Bundesamt für Polizei fedpol kommt eine Relais- und Filterfunktion zwischen den Finanzintermediären und den Strafverfolgungsbehörden zu. Sie ist die nationale Zentralstelle, welche gemäss dem Geldwäschereigesetz Verdachtsmeldungen bezüglich Geldwäscherei, Terrorismusfinanzierung, Gelder verbrecherischer Herkunft oder krimineller Organisationen von Finanzintermediären entgegennimmt, analysiert und allenfalls an die Strafverfolgungsbehörden weiterleitet.

Melde- und Analysestelle Informationssicherung (MELANI)[11]
Die Melde- und Analysestelle Informationssicherung (MELANI) ist vom Bundesrat mit dem Schutz der kritischen Infrastrukturen in der Schweiz beauftragt. Der Sinn und Zweck von MELANI ist sowohl die Früherkennung von Gefahren und deren Bewältigung sowie die Unterstützung der Betreiber von kritischen Infrastrukturen in Krisenzeiten. Die Website von MELANI richtet sich überdies an private Computer- und Internetnutzer sowie an kleinere und mittlere Unternehmen (KMU) der Schweiz. Um die Aktivitäten des Bundes im Bereich Cyberrisiken zu stärken, hat der Bundesrat am 30. Januar 2019 beschlossen, ein Kompetenzzentrum für Cybersicherheit zu errichten. Dieses soll auf bestehenden Kompetenzen und Fachstellen wie der gut etablierten MELANI aufgebaut werden. Im Bereich Phishing bietet MELANI die Möglichkeit, verdächtige E-Mails oder Webseiten zu melden.[12]

Schweizerische Kriminalprävention (SKP)[13]
Die SKP erarbeitet im Auftrag der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren thematische Präventionskampagnen, entwickelt Materialien und Projekte zur polizeilichen Präventionsarbeit und vernetzt die Polizei und ihre Kooperationspartner. Dabei spielt neben anderen Themen insbesondere auch die Betrugsprävention eine wichtige Rolle. Im Rahmen der polizeilichen Aus- und Weiterbildung ist die SKP zudem für die fachliche Betreuung der allgemeinen und der polizeilichen Prävention zuständig.

Plattform Coordination Food Fraud (COFF)[14]
Die Plattform COFF ist eine interdisziplinäre Arbeitsgruppe mit Vertretern des Bundesamtes für Landwirtschaft (BLW), der Eidgenössischen Zollverwaltung (EZV), fedpol, der kantonalen Lebensmittelvollzugsbehörden und des Bundesamtes für Lebensmittelsicherheit und Veterinärwesen (BLV). Sie ist für die Koordination der Bekämpfung von Lebensmittelbetrug zuständig. Das BLV ist das Kompetenzzentrum des Bundes für den Bereich Lebensmittelsicherheit und schafft unter anderem die Voraussetzungen, damit die Sicherheit von Lebensmitteln auf hohem Niveau gewährleistet werden kann und die Konsumentinnen und Konsumenten vor Täuschung geschützt sind. Es ist in Kooperation mit anderen Behörden an den nationalen Kontrollen von Produkten beteiligt.

Cyberboard
2018 ist das sogenannte *Cyberboard* geschaffen worden, das als schweizweite Plattform zur Koordination der Bekämpfung der Internetkriminalität fungiert. Involviert sind kantonale und nationale Strafverfolgungsbehörden sowie Akteure im Bereich der Prävention.

Netzwerk für die Ermittlungsunterstützung in der digitalen Kriminalität (NEDIK)
fedpol entlastet die Kantone durch die operative Koordination (inter-)nationaler und interkantonaler Fallkomplexe in Zusammenarbeit mit resp. als Mitglied des seit 2017 bestehenden „Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung“ (NEDIK). NEDIK wurde im Auftrag von der Konferenz der Kantonalen Polizeikommandanten der Schweiz (KKPKS) gegründet. NEDIK soll aus der Koordination der laufenden operativen Arbeiten aktuelle Arbeitsergebnisse zuhanden der Schweizer Polizei generieren. In einer ersten Phase geht es

[10] Siehe www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/geldwaescherei.html.
[11] Siehe www.melani.admin.ch.
[12] Siehe www.antiphishing.ch.
[13] Siehe www.skppsc.ch.
[14] Siehe https://www.blv.admin.ch/blv/de/home/lebensmittel-und-ernaehrung/lebensmittelsicherheit/verantwortlichkeiten/nationale-kontrollprogramme.html.

darum, die Zusammenarbeit der verschiedenen Zentren möglichst eng aufeinander abzustimmen, eine gemeinsame Fallübersicht zu gewinnen und neue Arbeitsprodukte zu entwickeln, welche allen Polizeibehörden einen Mehrwert bieten. fedpol hat innerhalb des NEDIK die Rolle der nationalen Zentralstelle und des nationalen Kompetenz- und Koordinationszentrums (siehe oben).

Strafverfolgungsbehörden
Die strafrechtliche Verfolgung von Betrug und betrügerischem Missbrauch einer Datenverarbeitungsanlage obliegt in der Schweiz in erster Linie den kantonalen Strafverfolgungsbehörden. Wirtschaftsdelikte werden dabei vielerorts in spezialisierten Einheiten behandelt, in denen das entsprechende Fachwissen vorhanden ist. Wenn die Straftaten zu einem wesentlichen Teil im Ausland oder in mehreren Kantonen begangen worden sind und dabei kein eindeutiger Schwerpunkt in einem Kanton besteht, können die Strafverfolgungsbehörden des Bundes im Bereich Wirtschaftskriminalität eigene Verfahren führen.[15] Im Bereich Abgabebetrug (Mehrwertsteuer, Verrechnungssteuer oder Stempelabgaben) werden Strafverfahren von der Eidgenössischen Steuerverwaltung oder, betreffend Mehrwertsteuer bei der Einfuhr von Waren, von der Eidgenössischen Zollverwaltung (EZV) geführt. Für diese Verfahren gilt das Verwaltungsstrafrecht.

2 Betrug als Straftatbestand

2.1 Betrug im Allgemeinen und Untersuchungsgegenstand

Umgangssprachlich steht Betrug für eine bewusste Täuschung in Verbindung mit einem Schaden für das Opfer und einem Vorteil für den Täter. Die umgangssprachliche Bedeutung geht weit über den strafrechtlichen Anwendungsbereich hinaus und kann für eine Vielzahl von Täuschungen verwendet werden. Diese sind äusserst vielfältig und haben sich mit den gesellschaftlichen und technischen Wandlungen weiterentwickelt. In seiner Betrugsklassifizierung unterscheidet der Forscher Levi beispielsweise die verschiedenen Betrugsformen nach dem Sektor (öffentlich vs. privat), Untersektor (Finanzdienstleitungen, nicht finanzielle Dienstleistungen, usw.) und der Aktivität des Opfers bzw. des Täters:[16]

[15] Gemäss Art. 24 Abs. 1 der Schweizerischen Strafprozessordnung (StPO) vom 5. Oktober 2007 (SR 312.0) ist die Bundesanwaltschaft zuständig, wenn die Geldwäschereihandlungen zu einem wesentlichen Teil im Ausland oder in mehreren Kantonen begangen worden sind und wenn dabei kein eindeutiger Schwerpunkt in einem Kanton besteht. Beim Betrug im Sinne von Art. 146 StGB bzw. beim Missbrauch einer DVA (Art. 147 StGB) ist die Bundesgerichtsbarkeit gegeben, wenn – neben den oben erwähnten Voraussetzungen – keine kantonale Strafverfolgungsbehörde mit der Sache befasst ist oder die zuständige kantonale Strafverfolgungsbehörde die Staatsanwaltschaft des Bundes um Übernahme des Verfahrens ersucht (Art. 24 Abs. 2 StPO).
[16] Levi, Michael (2008): *Organized fraud and organizing frauds. Unpacking research on networks and organization*, in: Criminology and Criminal Justice, 12.2008, S. 391.https://www.researchgate.net/profile/Michael_Levi4/publication/249786379_Organized_fraud_and_organizing_fraudsUnpacking_research_on_networks_and_organization/links/0c960532755df02414000000/Organized-fraud-and-organizing-fraudsUnpacking-research-on-networks-and-organization.pdf.

Tabelle 1: Klassifizierung von betrügerischen Delikten nach Levi (2008)

Opfer nach Sektor	*Opfer nach Untersektor*	*Beispiele von betrügerischen Delikten*
Privat	Finanzdienstleister	Checkbetrug
		Produktpiraterie
		Falschgeld
		Betrügerischer Missbrauch von Daten
		Veruntreuung
		Insiderhandel
		Versicherungsbetrug
		Kreditbetrug
		Missbrauch von Zahlungskarten
		Missbrauch im Beschaffungswesen
	Nicht-finanzielle Dienstleister	Checkbetrug
		Produktpiraterie
		Falschgeld
		Betrügerischer Missbrauch von Daten
		Veruntreuung
		Spielbetrug
		Kreditbetrug
		Missbrauch von Zahlungskarten
		Missbrauch im Beschaffungswesen
	Privatpersonen	Spendenbetrug
		Konsumentenbetrug
		Produktpiraterie
		Falschgeld
		Anlagebetrug
		Rentenbetrug
Öffentlich	Auf nationaler Ebene	Subventionsbetrug
		Veruntreuung (ungetreue Amtsführung)
		Missbrauch im Beschaffungswesen
		Steuerbetrug
	Auf lokaler Ebene	Veruntreuung (ungetreue Amtsführung)
		Steuerbetrug
		Missbrauch im Beschaffungswesen
	International	Missbrauch im Beschaffungswesen
		Betrug mit EU-Geldern (Subventionsbetrug)

Diese Klassifizierung ist nicht abschliessend und umfasst auch Betrugsvarianten, die nebst dem Straftatbestand von Art. 146 StGB[17] (wie z.B. Kredit-, Check- oder Anlagenbetrug) weitere

[17] Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (SR 311.0).

Straftatbestände erfüllen können (z.B. Steuerbetrug [Art. 59 StHG[18]; Art. 186 DBG[19]], Veruntreuung [Art. 138 StGB], usw.). Nicht jedes auf Täuschung basierendes Delikt eignet sich ausserdem als Vortat zur Geldwäscherei im Sinne von Art. 305bis StGB. Die Vermögenswerte müssen aus einem Verbrechen oder qualifizierten Steuervergehen stammen. Als Vortaten kommen somit in Frage – mit Ausnahme des qualifizierten Steuervergehens – Delikte, die mit Freiheitsstrafe von mehr als drei Jahren bedroht sind.[20] In Bezug auf den vorliegenden Bericht muss ausserdem das Element der vorsätzlichen Täuschung vorhanden sein. Diese zielt darauf ab, bei jemandem «eine von der Wirklichkeit abweichende Vorstellung hervorzurufen»[21]. Diese Täuschungshandlung ist elementarer Bestandteil jeder betrügerischen Handlung. Gemeinsam haben die nachfolgenden Tatbestände zudem, dass sie mehrstufig ausgestaltet sind. Es müssen also zur erfolgreichen Vollendung des jeweiligen Delikts mehrere Etappen durchlaufen werden. Dabei werden teilweise auch andere Straftaten wie beispielsweise Urkundendelikte begangen.

Dieser Bericht fokussiert auf zwei Straftaten: den Betrug im Sinne von Art. 146 StGB und den betrügerischen Missbrauch einer Datenverarbeitungsanlage (kurz: Missbrauch einer DVA) im Sinne von Art. 147 StGB. Dabei wird bei letzterer Straftat primär auf die Variante eingegangen, die auf Phishing basiert; andere Formen wie z.B. Skimming werden nicht weiter berücksichtigt.[22] Der Einfachheit halber werden diese beiden Straftaten in diesem Bericht unter den Begriff Betrugsdelikte subsumiert.

2.2 Betrug – Art. 146 StGB

Der Straftatbestand des Betrugs (Art.146 StGB) bedroht mit Freiheitstrafe von bis zu fünf Jahren, wer mit der Absicht einer ungerechtfertigten Bereicherung eine andere Person arglistig irreführt, indem er Tatsachen vorspiegelt oder unterdrückt, die das Opferdazu bringen, sich selber oder einen anderen am Vermögen zu schädigen. Handelt der Täter gewerbsmässig, so kann die Freiheitsstrafe bis zu zehn Jahren betragen.

Das Delikt besteht aus mehreren aufeinanderfolgenden Phasen oder Erfolgen, die sich realisieren müssen. Objektiv müssen somit bereits einige Voraussetzungen gegeben sein, damit Betrug gemäss Art. 146 StGB als Straftatbestand in Frage kommt. Die Irreführung kann einerseits durch eine unwahre Aussage (mündlich oder schriftlich) oder durch ein Unterdrücken von Tatsachen erfolgen. Sie muss ausserdem arglistig sein und einen Irrtum hervorrufen oder einen bestehenden Irrtum bestärken. Die getäuschte Person muss im Anschluss aufgrund des Irrtums eine Vermögensverschiebung vornehmen, welche bei ihr oder einer dritten Person einen Schaden hervorruft und somit den Betrüger oder eine dritte Person bereichert. Zwischen Schaden und Bereicherung muss ausserdem eine sogenannte Stoffgleichheit herrschen. Das heisst, der Vermögensnachteil der einen Person muss dem Vermögensvorteil der anderen entsprechen. Zwischen beiden ist ein innerer Zusammenhang notwendig.[23]

Mit der Arglist wird vom Geschädigten ein bestimmtes Mass an Selbstverantwortung verlangt. Gemäss Rechtsprechung des Bundesgerichts ist der Geschädigte insbesondere dann mitverantwortlich, wenn er sich mit einem Mindestmass an zumutbarer Sorgfalt selbst hätte schützen können oder wenn er die grundlegendsten Vorsichtsmassnahmen nicht beachtet hat.[24] In diesen Fällen ist der Tatbestand des Betrugs nicht erfüllt. Grundsätzlich ist Arglist hingegen immer

[18] Bundesgesetz über die Harmonisierung der direkten Steuern der Kantone und Gemeinden (StHG) vom 14. Dezember 1990 (SR 642.14).
[19] Bundesgesetz über die direkte Bundessteuer (DBG) vom 14. Dezember 1990 (SR 642.11).
[20] Art. 10 Abs. 2 StGB.
[21] Trechsel, Stefan / Crameri, Dean (2012): *Art. 146 Betrug*, in: Trechsel, Stefan / Pieth, Mark (Hrsg.): Schweizerisches Strafgesetzbuch Praxiskommentar, 2. Aufl., Zürich 2012, S. 739.
[22] Beim Skimming handelt es sich um das Manipulieren von Kartenautomaten anhand gestohlener oder illegal kopierter Konto-, Debit oder Kreditkarten, mit dem Ziel Geld abzuheben.
[23] BGE 134 IV 210, E. 5.3, S. 213.
[24] BGE 126 IV 165, E. 2, S. 171–172.

dann gegeben, wenn besondere Machenschaften[25] angewandt werden oder ein Lügengebäude[26] errichtet wird. Unter gewissen Voraussetzungen kann auch eine einfache Lüge arglistig sein. Dies trifft zu, wenn die Überprüfung der Lüge für den Betrogenen entweder nicht oder nur mit besonderer Mühe möglich ist bzw. nicht zugemutet werden kann, die Überprüfung vom Betrüger absichtlich verhindert wird oder wenn aufgrund eines besonderen Vertrauensverhältnisses zu erwarten ist, dass der Betrogene die Überprüfung unterlassen wird. Somit ist der Tatbestand nur anwendbar, wenn die vorgespiegelten oder unterdrückten Tatsachen für das Opfer schwer oder gar nicht überprüfbar sind. Dabei sind stets die Fähigkeiten des Geschädigten oder die besonderen Umstände zu berücksichtigen, welche dem Opfer die Überprüfung erschweren oder erleichtern.[27]

In subjektiver Hinsicht muss bei allen objektiven Tatbestandsmerkmalen Vorsatz (Eventualvorsatz genügt) gegeben sein. Die Bereicherungsabsicht muss beim Täter bereits in der Phase des Irrtums bestehen. Ausserdem muss ein Motivationszusammenhang zwischen Irreführung, Irrtum und Vermögensdisposition vorhanden sein.

2.3 Betrügerischer Missbrauch einer Datenverarbeitungsanlage - Art. 147 StGB

Art. 147 StGB bestraft denjenigen, der in der Absicht sich oder einen Dritten unrechtmässig zu bereichern, Daten unrichtig, unvollständig oder unbefugt verwendet oder in vergleichbarer Weise auf einen elektronischen oder vergleichbaren Datenverarbeitungs- und Datenübermittlungsvorgang einwirkt. Voraussetzung ist auch hier, dass eine Vermögensverschiebung stattfindet, die bei einem Dritten einen Schaden hervorruft.

In subjektiver Hinsicht bestehen ausser dem Vorsatz und der Bereicherungsabsicht keine weiteren Anforderungen. Zu beachten ist lediglich, dass wie beim Betrug zwischen Schaden und Bereicherung Stoffgleichheit bestehen muss.[28]

Im Unterschied zum Betrug gemäss Art. 146 StGB wird hier nicht ein Mensch getäuscht, sondern (im übertragenen Sinn) eine Maschine. Mit der Schaffung des Tatbestands hat der Gesetzgeber eine durch die technische Entwicklung entstandene Gesetzeslücke geschlossen. Denn der sogenannte Computerbetrug konnte nicht unter Art. 146 StGB subsumiert werden, da eine Maschine keinem Irrtum i.S.v. Art. 146 StGB erliegen und dementsprechend auch nicht getäuscht werden kann.[29] Gemäss Botschaft sollten Handlungen unter Strafe gestellt werden, «bei denen zum Zweck der unrechtmässigen Bereicherung mittels der Manipulation von Daten oder Datenverarbeitungsanlagen diese zu einer Vermögensverschiebung veranlasst werden, die bei korrekter Handhabung nicht stattgefunden hätte».[30]

Die sogenannten Computerdelikte wurden analog zu den bestehenden Straftatbeständen konzipiert, sodass der betrügerische Missbrauch einer Datenverarbeitungsanlage an den Betrug im Sinne von Art. 146 StGB angelehnt ist. Das Einwirken auf den Datenverarbeitungs- oder Datenübermittlungsvorgang ist mehr oder weniger das Pendant der arglistigen Täuschung

[25] Von Machenschaften spricht man, wenn bspw. gefälschte Belege oder Urkunden eingesetzt werden, um die gemachten Aussagen glaubwürdig erscheinen zu lassen.
[26] Ein Lügengebäude erfordert mehrere raffiniert aufeinander abgestimmte Lügen, welche von besonderer Hinterhältigkeit zeugen, sodass sich auch ein kritisches Opfer täuschen lässt (BGE 135 IV 76, 81). Mehrere einzelne Lügen reichen nicht aus.
[27] Urteil (des Bundesgerichts) 6P.172/2000 und 6S.776/2000 vom 14.5.2001, E. 8. Solche Umstände können bspw. bei geistesschwachen, unerfahrenen oder aufgrund des Alters oder einer Krankheit beeinträchtigten Opfern gegeben sein sowie in denjenigen Fällen, in denen ein Abhängigkeits- oder Unterordnungsverhältnis besteht oder sich das Opfer in einer Notlage befindet, welches ihr Misstrauen gegenüber dem Täter einschränkt. Demgegenüber sind besondere Fachkenntnisse und die Geschäftserfahrung des Opfers ebenfalls zu berücksichtigen.
[28] Siehe Fiolka, Gerhard (2019): *Art. 147*, in: Niggli, Marcel Alexander / Wiprächtiger, Hans (Hrsg.): Strafrecht II, Art. 111–392 StGB. Basler Kommentar, 4. Aufl., Basel 2019, S. 3173.
[29] Siehe Fiolka (2019), op. cit. S. 3162 f.
[30] Bundesrat (1991): Botschaft über die Änderung des Schweizerischen Strafgesetzbuches und des Militärstrafgesetzes (Strafbare Handlungen gegen das Vermögen und Urkundenfälschung) sowie betreffend die Änderung des Bundesgesetzes über die wirtschaftliche Landesversorgung (Strafbestimmungen) vom 24. April 1991, BBl 1991 II 1020.

beim Betrug. Als Ergebnis der Einwirkung auf die Datenverarbeitung oder -übermittlung wird eine Vermögensdisposition zugunsten der falschen Person bewirkt. Wie der Täter an die dafür notwendigen Daten gelangt ist, spielt dabei keine Rolle.[31]

2.4 Weitere, betrugsähnliche Delikte

Wie bereits erwähnt, konzentriert sich der vorliegende Bericht auf die Geldwäschereivortaten Betrug und Phishing zwecks dem betrügerischen Missbrauchs einer DVA. Andere Delikte, die zwar auch Elemente der Täuschung beinhalten, werden im vorliegenden Bericht nicht behandelt, da diese einerseits nicht vom Berichtsauftrag erfasst sind und andererseits meistens als Vergehen keine Vortat zur Geldwäscherei darstellen, oder, wenn schon, nur in ihrer qualifizierten Form. Andere Straftaten mit Täuschungskomponenten sind zudem oft an Voraussetzungen oder objektive Strafbarkeitsbedingungen geknüpft, die beispielsweise den Täter- oder Opferkreis einschränken oder die Eröffnung des Konkurses bedingen. Beispiele hierfür sind insbesondere Börsen-, aber auch Konkurs- und Vermögensdelikte, die als Vergehen ausgestaltet sind. Anhand zweier Beispiele wird nachfolgend dargestellt, welche Parallelen und Unterschiede zwischen solchen Delikten und dem Betrug nach Art. 146 StGB bestehen.

In Art. 163 regelt das StGB den betrügerischen Konkurs und Pfändungsbetrug. Im Wesentlichen beinhaltet der Straftatbestand eine Täuschungshandlung des Schuldners oder eines Dritten über die vorhandenen Aktiven und Passiven zum Zeitpunkt des Konkurses. Der betrügerische Konkurs und Pfändungsbetrug kommt als Geldwäschereivortat aber nur dann in Frage, wenn der Täter zugleich Schuldner ist.[32] Als objektive Strafbarkeitsbedingung ist die Eröffnung des Konkurses oder Ausstellung eines Verlustscheins vorausgesetzt. Geschädigt wird somit ausschliesslich der Gläubiger. Als geschütztes Rechtsgut gelten deren Ansprüche im Konkurs- und Betreibungsverfahren (im Gegensatz zum Vermögen beim Betrug). Häufig begeht der Täter in der Ausführung dieses Delikts Urkundendelikte, was wiederum beim Betrug auch vorkommen kann.[33] Zwar ist auch beim betrügerischen Konkurs und Pfändungsbetrug die Täuschungshandlung ein wesentlicher Aspekt des Straftatbestands, im Gegensatz zu Art. 146 StGB besteht aber zusätzlich zur objektiven Strafbarkeitsbedingung eine deutliche Einschränkung des Täter- und Geschädigtenkreises.

Im Bereich der Steuern gelten der qualifizierte Leistungs- und Abgabebetrug sowie das qualifizierte Steuervergehen als Geldwäschereivortaten. Der Karussellbetrug im Bereich der Mehrwertsteuer gilt als Betrug im Sinne von Art. 146 StGB (cf. infra). Der qualifizierte Leistungs- und Abgabebetrug[34] ist in der Schweiz bereits seit 2009 als Vortat zur Geldwäscherei anerkannt. Bis Ende 2015 galt dieser Tatbestand jedoch nur für den grenzüberschreitenden Warenverkehr und beschränkte sich damit auf den Zollschmuggel. Im Zuge der Umsetzung der revidierten GAFI-Empfehlungen[35] wurde der qualifizierte Abgabebetrug dahingehend erweitert, dass die Bestimmung neu auch auf in der Schweiz im Abgabebereich begangene Straftaten anwendbar ist. Der Tatbestand umfasst somit seit dem 1. Januar 2016 auch die Verrechnungssteuer, die Mehrwertsteuer, Stempelabgaben, Lieferungen im Inland, die Erbringung von Dienstleistungen sowie die Alkohol- und Tabaksteuer bei inländischer Herstellung.[36] Darüber hinaus erfordert der Tatbestand analog zum Betrug arglistiges Irreführen oder arglistiges Bestärken in einem Irrtum.

---

[31] Siehe Fiolka (2019), op. Cit. S. 3164.
[32] Wenn ein Dritter (nicht der Schuldner) der Täter ist, beträgt die Strafandrohung maximal drei Jahre. Der Straftatbestand ist in diesem Fall keine Geldwäschereivortat.
[33] Brunner, Alexander (2007): *Art. 163*, in: Niggli, Marcel Alexander / Wiprächtiger, Hans (Hrsg.): Strafrecht II, Art. 111–392 StGB. Basler Kommentar, 2. Aufl., Basel 2007, S. 785–797.
[34] Art. 14 Abs. 4 des Bundesgesetzes vom 22. März 1974 über das Verwaltungsstrafrecht VStrR (SR 313.0).
[35] Vgl. Bundesgesetz zur Umsetzung der 2012 revidierten Empfehlungen der Groupe d'action financière vom 12. Dezember 2014 (AS 2015 1389).
[36] Bundesrat (2013): Botschaft zur Umsetzung der 2012 revidierten Empfehlungen der GAFI vom 13.12.2015, BBl 2014 605.

Das qualifizierte Steuervergehen wurde 2016 mit der Umsetzung der revidierten GAFI-Empfehlungen in Art. 305bis Abs. 1bis StGB zur Geldwäschereivortat erhoben. Vorausgesetzt wird ein Steuerbetrug[37], das heisst die Verwendung von gefälschten, verfälschten oder unwahren Urkunden zur Täuschung der Steuerbehörde zwecks Begehung einer Steuerhinterziehung. Die hinterzogenen Steuern müssen dabei mehr als 300'000 Franken pro Steuerperiode betragen.

Der Leistungs- und Abgabe- sowie der Steuerbetrug stellen somit im Unterschied zum Betrug nur in ihrer qualifizierten Form eine Geldwäschereivortat dar.

3 Gefährdung ausgehend vom Betrug und dem betrügerischen Missbrauch einer Datenverarbeitungsanlage als Vortat zur Geldwäscherei

3.1 Allgemeine Gefährdung

Gemäss der GAFI geht eine Bedrohung von einer Person, einer Gruppe von Personen, einer Sache oder einer Handlung aus, die beispielsweise dem Staat oder der Gesellschaft schaden könnte.[38] So kann eine Straftat eine Gefährdung bilden. Jeder erfolgreiche Betrug im strafrechtlichen Sinn und jeder erfolgreiche betrügerische Missbrauch einer DVA stellt eine mögliche Vortat zur Geldwäscherei und somit eine potenzielle Geldwäschereigefahr dar. Vorausgesetzt wird lediglich, dass diese nicht als geringfügige Vermögensdelikte im Sinne des Art. 172ter StGB eingestuft werden, denn diese können keine Vortat zur Geldwäscherei bilden. Als geringfügig gelten in der Regel nicht gewerbsmässig durchgeführte Taten, die mit einer Busse geahndet werden und einen Vermögenswert oder Schaden von bis zu 300 Franken betreffen.[39] Reine Betrugsversuche scheiden als Vortat zur Geldwäscherei ebenfalls aus, da es üblicherweise in diesem Stadium noch keine zu waschenden Vermögenswerte geben kann. Wie bei vielen anderen Delikten ist beim Betrug und beim Missbrauch einer DVA von einem hohen Dunkelfeld auszugehen. Die Dunkelziffer hat beim Betrug vielfältige Gründe: Ein Opfer dürfte gar nicht immer bemerken, dass es betrogen wurde (im Gegensatz beispielsweise zum Diebstahl). Zudem verzichten einige Personen aus Scham auf eine Anzeige, Unternehmen fürchten unter Umständen einen allfälligen Reputationsschaden. Schliesslich sind Vermögenswerte, die durch einen Betrug entwendet werden, in der Regel nicht versichert (im Gegensatz zu vielen Diebstählen, wo das Vorliegen einer Anzeige vom Versicherer verlangt werden kann). Hinweise zur Prävalenz der Betrugsdelikte liefern die sogenannten Opferbefragungen. Die Polizeiliche Kriminalstatistik (PKS), die Strafurteilstatistik (SUS), die Verdachtsmeldungen an die MROS und die Meldungen im Bereich Internetkriminalität an fedpol liefern weitere Hinweise hinsichtlich der Art und Häufigkeit betrügerischer Vermögensdelikte in der Schweiz. Letztere Statistiken begrenzen sich allerdings auf das Hellfeld, das heisst auf die Straftaten, von denen die Strafbehörden Kenntnis erhalten haben.

3.1.1 Opferbefragungen

Eine der umfangreichsten Opferbefragungen in der Schweiz ist die Studie zur Kriminalität und Opfererfahrungen der Schweizer Bevölkerung von Biberstein et al., die im Auftrag der Konferenz der Kantonalen Polizeikommandanten der Schweiz (KKPKS) zum letzten Mal 2015 durchgeführt wurde.[40] In dieser Studie wurden unter anderem Fragen gestellt, mit dem Ziel die Prävalenz von den Deliktskategorien «Verbraucherschwindel», «Missbrauch von Kredit- oder Bankkundenkarte» und «Übergriff im Internet» (inkl. Phishing) zu eruieren. Diese Delikte ent-

[37] Vgl. Art. 186 DBG, Art. 59 Abs. 1 StHG und Art. 305bis Abs. 1bis StGB.
[38] GAFI (2013), op. cit., S. 7.
[39] Vgl. Weissenberger, Philippe (2019): *Art. 172ter*, in: Niggli, Marcel Alexander / Wiprächtiger, Hans (Hrsg.): Strafrecht II, Art. 111–392 StGB. Basler Kommentar, 4. Aufl., Basel 2019, S. 3550-3563.
[40] Biberstein et al. (2016): Studie zur Kriminalität und Opfererfahrungen der Schweizer Bevölkerung. Analysen im Rahmen der schweizerischen Sicherheitsbefragung 2015.

sprechen am ehesten den Tatbeständen des Betrugs und des Missbrauchs einer DVA. Damals gaben 8,5% der Befragten an, innerhalb der letzten fünf Jahre Opfer eines Verbraucherschwindels gewesen zu sein. Beim Missbrauch von Kredit- oder Bankkundenkarten lag dieser Wert 2015 bei 3,5% und bei den Übergriffen im Internet bei 6,6%. 2011 erreichte die Prävalenz 10,5% (Verbraucherschwindel) und 2,7% (Kreditkartenmissbrauch). Die Studie wertete auch das Anzeigeverhalten der Opfer aus. Bei den drei obenerwähnten Deliktskategorien erstatteten damals 10,5% (Verbraucherschwindel), 23% (Kreditkartenmissbrauch) bzw. 3,9% (Übergriffe im Internet) der Befragten Anzeige.[41]

Beaudet-Labrecque et al. untersuchten 2018 in einer schweizerischen Studie die finanziellen Missbräuche bei Personen ab 55 Jahren.[42] Über ein Viertel der Befragten (28,3%) gaben an, innerhalb der letzten fünf Jahren Opfer von diversen Betrugsversuchen gewesen zu sein (bei Cyberkriminalität: 27,8%). Bei 6,6% wurde der Betrug vollendet (Cyberkriminalität: 3,1%).[43] Basierend auf dieser Umfrage rechneten die Autoren der Studie hoch, wie viele Personen ab 55 Jahren in den letzten fünf Jahren mit diesen Betrugsarten bzw. mit Internetkriminalität konfrontiert worden sind bzw. wie viele dadurch einen finanziellen Verlust erlitten haben. Am häufigsten waren demgemäss Versuche mit Phishing (Hochrechnung: 594'421 betroffene Personen ab 55 Jahren), Vorschussbetrug (387'666), mit dem sogenannten «Unbekannten in Not»-Trick[44] (234'753) und im Bereich Anlagebetrug (202'448). Zu finanziellem Schaden kamen Personen vor allem wegen dem «Unbekannten in Not»-Trick (60'304), gefälschten Anzeigen im Internet (47'381), dem Währungstausch (23'691) und Romance/Love Scamming (15'076).[45] Der durchschnittliche finanzielle Schaden lag bei der Cyberkriminalität bei 6'437 Franken (Medianverlust: 400 Fr.) und bei den verschiedenen Betrugsarten bei 2'100 Franken (Medianverlust: 200 Fr.).[46]

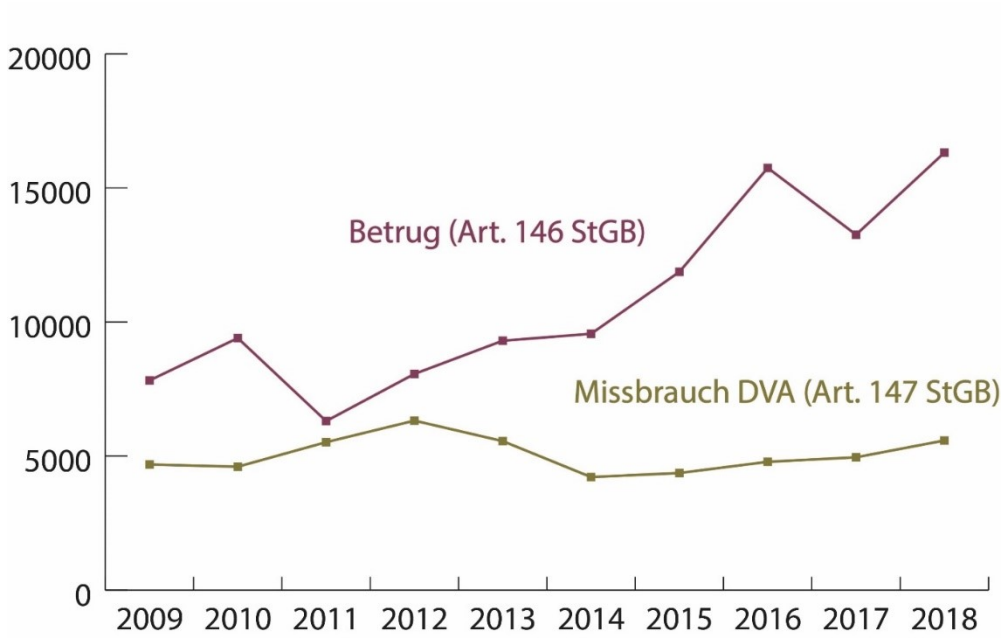
In einer von PwC 2017 durchgeführten Umfrage zur Wirtschaftskriminalität gaben 39% der befragten Schweizer Unternehmer an, innerhalb der letzten zwei Jahre Opfer eines Betrugs oder eines anderen Wirtschaftsdelikts geworden zu sein. Am meisten meldeten die betroffenen Firmen als Deliktart die Veruntreuung von Vermögenswerten (51%), Cyberkriminalität (44%), Geschäfts(fehl)verhalten (31%) und vom Verbraucher begangener Betrug (23%). Bei der Cyberkriminalität waren das Phishing und das Einsetzen von Malware die zwei am häufigsten verwendeten Techniken (42% bzw. 31%). Der durchschnittliche unmittelbare Schaden der Wirtschaftskriminalität betrug 9,5 Millionen Franken.[47]

Opferbefragungen zeigen, dass die Betrugsdelikte in ihrer Gesamtheit viele natürliche und juristische Personen in der Schweiz betreffen und dass die Dunkelziffer vergleichsweise hoch ist. Allerdings legen sie auch dar, dass der Schaden bei natürlichen Personen in der Mehrheit der Fälle verhältnismässig gering ist. Somit könnten die Straftaten unter Umständen als geringfügige Vermögensdelikte eingestuft werden und würden demnach nicht als Vortat zur Geldwäscherei fungieren. Höhere Summen betreffen vor allem juristische Personen. Die Daten aus den Opferbefragungen, vor allem diejenigen der natürlichen Personen, sind aber nicht ausreichend, um die zeitliche Entwicklung der Betrugsdelikte auszuwerten. Ausserdem liefern solche Befragung keine Informationen zu Betrugsfällen, bei welchen die Geschädigten zwar

[41] Ibd., S. 16-21.
[42] Am 31.12.2018 betrug die Anzahl Personen ab 55 Jahren aus der ständigen Wohnbevölkerung der Schweiz 2,6 Millionen (31.5% der gesamten ständigen Wohnbevölkerung).
[43] Beaudet-Labrecque et al. (2018a): Finanzieller Missbrauch. Nationale Studie zur Untersuchung der Betrugsarten in der Altersgruppe 55+, S. 15-16. https://www.prosenectute.ch/dam/jcr:e0a731a4-ab86-4810-b10c-e4f532374ad4/Finanzieller-Missbrauch-Studienbericht-01.10.2018.pdf.
[44] Eine Art von Spendenbetrug, siehe auch Kapitel 3.2.3.
[45] Beaudet-Labrecque et al. (2018b) : «Finanzieller Missbrauch» - häufigste Betrugsarten in der Schweiz. https://www.prosenectute.ch/dam/jcr:7d5c59ff-5b6b-468c-8666-3a6d21abe729/Finanzieller-Missbrauch-haeufigste-Betrugsformen-in-der-Schweiz-01.10.2018.pdf.
[46] Beaudet-Labrecque et al. (2018a), op. cit., S. 15-16.
[47] PricewaterhouseCoopers (2018): Gesunken, aber nicht geschlagen: Schweizer Wirtschaftskriminelle werden digital und suchen sich neue Tätigkeitsfelder. Globale Umfrage zur Wirtschaftskriminalität 2018 – Schweizer Erkenntnisse, S. 4-11. https://www.pwc.ch/de/publications/2018/globale-umfrage-zur-wirtschaftskriminalitaet-2018.pdf.

im Ausland sitzen, aber die zu waschenden Vermögenswerte in die Schweiz transferiert werden.

3.1.2 Polizeiliche Kriminalstatistik (PKS)



Grafik 1: Von der Polizei verzeichnete Betrugsfälle sowie betrügerische Missbräuche einer Datenverarbeitungsanlage seit 2009. Quelle: Bundesamt für Statistik.

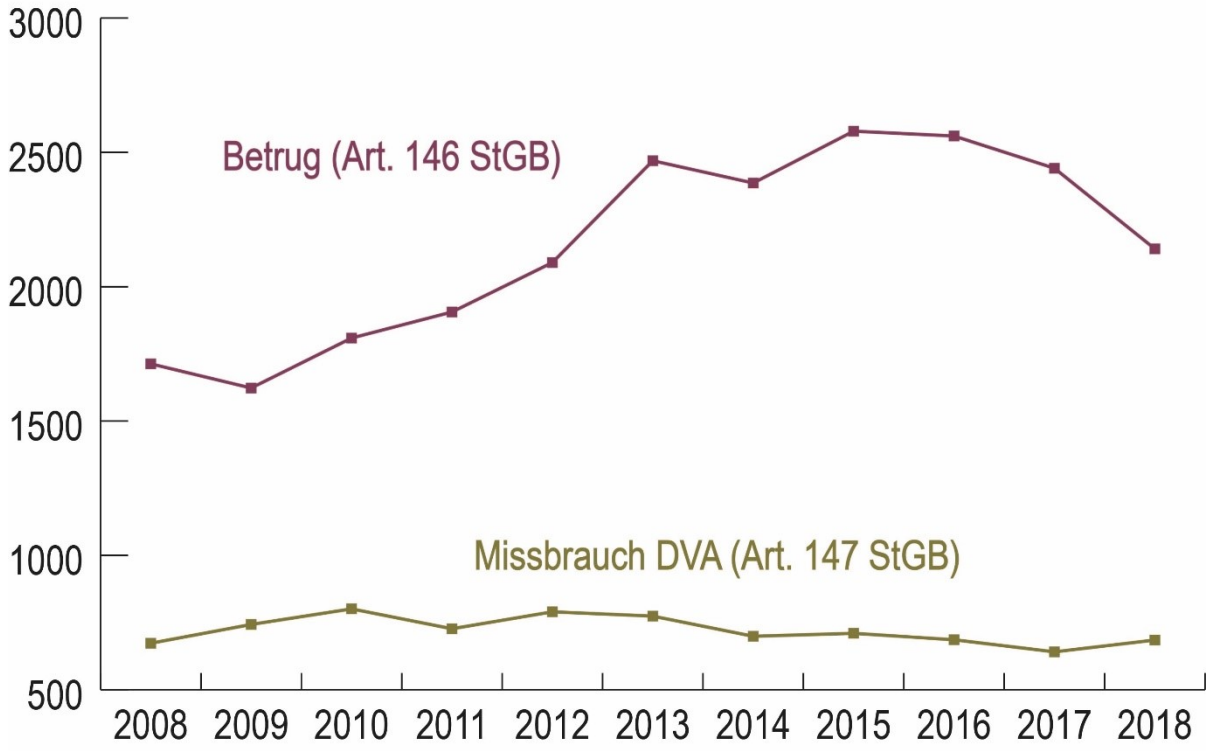
Die polizeiliche Kriminalstatistik (PKS) wird seit 2009 vom Bundesamt für Statistik (BFS) erstellt und erfasst sämtliche von der Polizei registrierten Straftaten. Die Anzahl der dort verzeichneten Betrüge und Missbräuche einer DVA weisen in den letzten zehn Jahren unterschiedliche Entwicklungen aus. Mit 16'319 gemeldeten Straftaten im Jahr 2018 hat sich die Anzahl Betrüge seit 2009 mehr als verdoppelt.[48] Die Missbräuche einer DVA sind dagegen im selben Zeitraum trotz einer leichten Zunahme seit 2014 tendenziell stabil geblieben.[49] 2018 betrug ihre Anzahl 5'538. Grundsätzlich sind die urban geprägten Kantone proportional stärker betroffen: Basel-Stadt (Häufigkeitszahlen im Jahr 2018 beim Betrug 5,7‰ und beim Missbrauch DVA 1,6‰), Genf (3,2‰/1,7‰) und Zürich (2,6‰/0,9‰). Am wenigsten Straftaten pro Einwohner hatten die Kantone Appenzell Innerrhoden (0.9‰/<0.2‰)[50], Appenzell Ausserrhoden und Uri (beide 1‰/<0.2‰).[51] 2018 waren 85,8% der gemeldeten Betrüge bzw. Missbräuche DVA 89,9% vollendet. Diese hohen Erfolgsquoten sind höchstwahrscheinlich darauf zurückzuführen, dass die überwiegende Mehrheit der Betrugs- und Missbrauchsversuche nicht angezeigt werden. Für die Bewertung des Geldwäschereirisikos sind allerdings nur die erfolgten Straftaten relevant. Die Aufklärungsquote lag 2018 beim Betrug bei 50,5% und beim Missbrauch einer DVA bei 31,1%. Da nur die Fälle berücksichtigt werden können, die auch im gleichen Jahr polizeilich aufgeklärt wurden, dürfte die tatsächliche Aufklärungsquote eigentlich etwas höher liegen. Insgesamt wurden 2018 4'875 Person des Betrugs und 1'348 des Missbrauchs einer DVA beschuldigt. Vier Fünftel (81,7%) gehörten beim Betrug der ständigen Wohnbevölkerung an (Schweizer und Ausländer mit B- oder C-Ausweis). Dieser Anteil war beim Missbrauch einer DVA etwas tiefer (73,2%). Die grosse Mehrheit der Tatverdächtigen

[48] Zu beachten ist allerdings die Tatsache, dass ein einziger Betrugsfall mehrere Straftaten erfassen kann und somit die Statistik stark beeinflussen kann, wie beispielsweise 2016 im Kanton Aargau (3920 Straftaten für einen einzigen Fall).
[49] Die Abnahme zwischen 2012 und 2014 liegt vermutlich am Rückgang der sogenannten Skimmingfälle infolge technischer Ausrüstung und besserer Kontrollmechanismen.
[50] In diesem Kanton wurde 2018 eine einzige Straftat wegen Missbrauch einer DVA verzeichnet.
[51] Bundesamt für Statistik (2019d): Polizeiliche Kriminalstatistik (PKS). Jahresbericht 2018 der polizeilich registrierten Straftaten, S. 18. https://www.bfs.admin.ch/bfsstatic/dam/assets/7726191/master.

waren Männer (71,4% beim Betrug und 73,2% beim Missbrauch einer DVA). 59,9% aller wegen Betrug Beschuldigten waren zwischen 20 und 44 Jahre alt (Missbrauch einer DVA 62,5%).

Die PKS zeigt zusammengefasst, dass die gemeldeten Betrugsfälle tendenziell zunehmen, die Zahlen beim Missbrauch einer DVA aber eher stabil bleiben. Die urban geprägten Kantone sind sowohl in absoluten als auch in relativen Zahlen am stärksten betroffen. Die meisten Tatverdächtigen sind Männer im mittleren Alter und in der Schweiz wohnhaft. Es werden in erster Linie erfolgreich durchgeführte Straftaten angezeigt. Insgesamt bildeten diese zwei Straftatbestände aber nur 7,6% aller im Jahr 2018 verzeichneten Vermögensdelikte in der Schweiz. Der weitaus grösste Teil aller Anzeigen in diesem Bereich sind nach wie vor Diebstahlsdelikte (2018: 59%). Allerdings ist wie bereits erwähnt beim Betrug von einem besonders hohen Dunkelfeld auszugehen.

3.1.3 Strafurteilsstatistik (SUS)



Grafik 2: Verurteilungen wegen Betrug und betrügerischen Missbrauchs einer Datenverarbeitungsanlage in der Schweiz seit 2008. Quelle: Bundesamt für Statistik

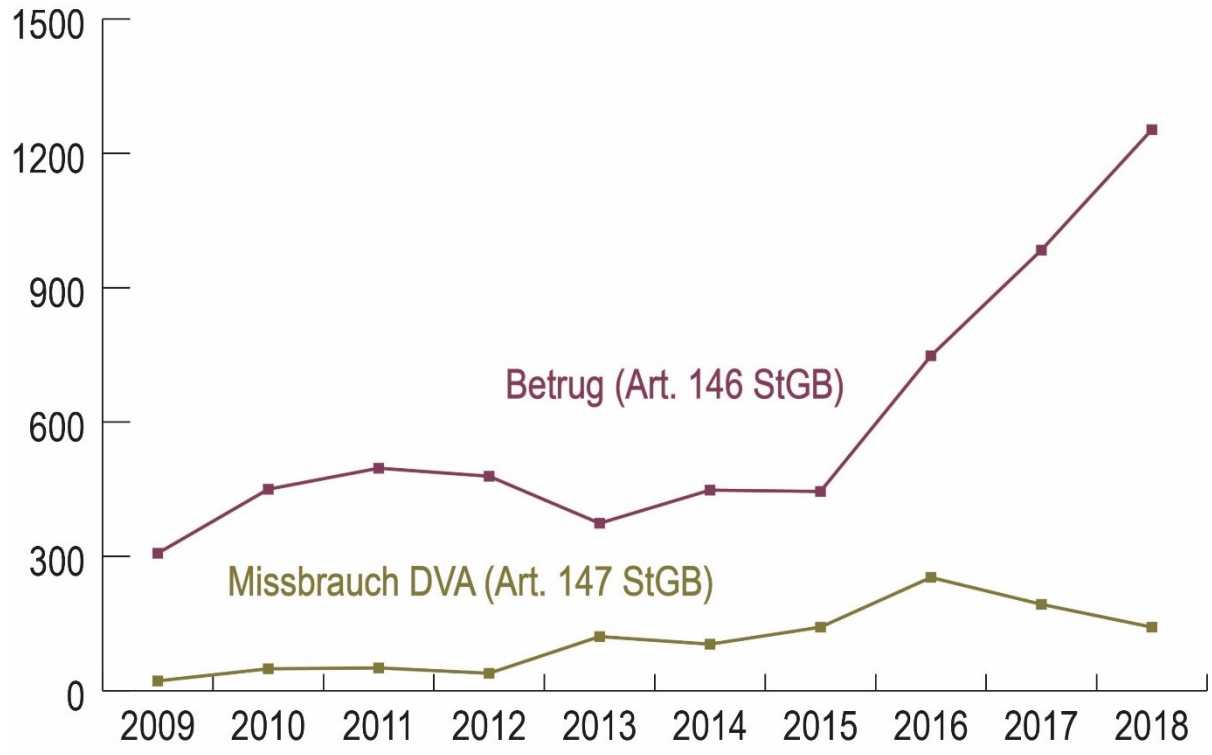
Die Strafurteilsstatistik (SUS) besteht in ihrer heutigen Form seit 1984. Sie weist alle ins Strafregister eingetragenen rechtskräftigen Verurteilungen von Erwachsenen und Minderjährigen aus, die aufgrund eines Verbrechens oder Vergehens ausgesprochen wurden.

Nach einer Zunahme zwischen 2009 und 2015 (mit einem Aussetzer 2014) geht die Anzahl Verurteilungen wegen Betrugs grundsätzlich zurück. Sie lag 2018 bei 2'141 Verurteilungen (2015: 2'579). Die Verurteilungen wegen Missbrauch einer DVA pendeln seit zehn Jahren zwischen rund 600 und 800 Urteilen pro Jahr (2018: 685). Vor allem beim Betrug kontrastiert die Entwicklung in der SUS dem beobachteten Anstieg in der PKS. Zudem sind bei der SUS die Zahlen deutlich tiefer als bei der PKS. Dies liegt zum einen daran, dass die Strafurteilsstatistik der aktuellen Lage immer hinterherhinkt, da sich die Verfahren bis zur rechtskräftigen Verurteilung, insbesondere im Bereich Wirtschaftskriminalität, teils über mehrere Jahre hinziehen können. Ausserdem führt nicht jede angezeigte Straftat zu einer Verurteilung; andersrum können verschiedene vom gleichen Täter durchgeführte Verbrechen oder Vergehen in ein einzi-

ges Strafurteil münden. Es ist zudem anzunehmen, dass kleineren Täterkreisen dank der neueren Informations- und Kommunikationstechnologien (IKT) immer mehr Möglichkeiten zur Verfügung stehen, um viele Opfer zu betrügen. Weiter weisen viele Betrugsfälle, insbesondere Phishing zwecks Missbrauch einer DVA, die mithilfe der IKT durchgeführt werden, einen Auslandbezug aus (cf. unter anderem Unterkapitel 4.1.5). Sie können unter Umständen von ausländischen Strafverfolgungsbehörden übernommen werden, wenn dort bereits ein Verfahren gegen die Täterschaft läuft. Übertretungen aufgrund geringfügiger Vermögensdelikte sind ferner in der Statistik nicht erfasst. Letztlich kann sich im Verlauf eines Verfahrens wegen Betrug ergeben, dass nicht der Tatbestand des Betrugs, sondern ein anderer erfüllt ist, sodass letztendlich beispielsweise ein Schuldspruch wegen Veruntreuung oder Urkundenfälschung erfolgt.

Verurteilungen wegen Betrug und betrügerischem Missbrauch einer DVA machten 2018 rund 15,7% aller Verurteilungen wegen Vermögensdelikten aus. Wie bei der PKS bildeten die Diebstähle die grösste Deliktskategorie (45,9%) in diesem Bereich.

3.1.4 Verdachtsmeldungen MROS



Grafik 3: Verdachtsmeldung an die MROS mit vermuteter Vortat Betrug und betrügerischem Missbrauch einer Datenverarbeitungsanlage seit 2009. Quelle: MROS.

Die Verdachtsmeldungen an MROS geben Auskunft über die vermuteten Vortaten zur Geldwäscherei. Da Finanzintermediäre angehalten sind, bei einem Verdacht unmittelbar eine Verdachtsmeldung abzusetzen, sind die Meldungen ein guter und aktueller Indikator für die Vortaten zur Geldwäscherei. Beachtet werden muss aber, dass Geldwäschereihandlungen ohne Einbezug von Finanzintermediären nicht in dieser Statistik enthalten sind. Ausserdem erweist sich im Nachhinein nicht jeder Verdacht als begründet; in manchen Fällen dürfte Betrug auch als eine Art Auffangtatbestand dienen. Präsentiert wird hier die statistische Auswertung der Verdachtsmeldungen, die in den zehn letzten Jahren (2009-2018) an MROS übermittelt worden sind.

Betrug ist mit durchschnittlich 24,4% die am häufigsten vermutete Vortat bei den an MROS adressierten Verdachtsmeldungen der letzten zehn Jahre.[52] Der betrügerische Missbrauch einer DVA machte rund 5% aller Meldungen aus. Zwischen 2015 und 2018 hat sich die Anzahl Meldungen mit Betrug als vermutete Vortat von 445 auf 1'253 fast verdreifacht (+182%). Diese Zunahme ist proportional stärker als diejenige, die bei allen Verdachtsmeldungen im gleichen Zeitraum beobachtet wird (+160%, von 2'367 auf 6'144). Über vier Fünftel (84,3%) aller Verdachtsmeldungen zwischen 2009 und 2018 im Zusammenhang mit Betrug kamen aus dem Bankensektor; in erster Linie aus Grossbanken (27,7% aller Meldungen) und aus ausländisch beherrschten Banken (17,6%). Bei den anderen Kategorien von Finanzintermediären waren zahlenmässig vor allem Zahlungsverkehrsdienstleister (7,5% aller Meldungen), Treuhänder (2%), Vermögensverwalter (1,8%) und Versicherungen (1,7%) von Bedeutung. Bei dem betrügerischen Missbrauch einer DVA kamen in der gleichen Zeitspanne noch mehr Verdachtsmeldungen aus dem Bankensektor (93,7%). Auch in diesem Bereich haben vor allem Grossbanken (26,3%) Meldung erstattet. Weitere übliche Melder waren Kantonalbanken (16,1%) und Raiffeisenbanken (13,7%). Bei den anderen Typen von Finanzintermediären kamen insbesondere Zahlungsverkehrsdienstleister (5%) in Betracht. Wie bei anderen Vortaten stammen die meisten Meldungen vor allem aus dem Bankensektor, was auf die in diesem Bereich vergleichsweise hohe Anzahl Kunden zurückzuführen ist. Zudem erhalten Banken Swift-Nachrichten, die unter Umständen zu einem Geldwäschereiverdacht führen können.

Sowohl beim Betrug als auch beim Missbrauch einer DVA konzentrierten sich über vier Fünftel aller verdächtigen Geschäftsbeziehungen in vier Kantonen: Zürich (39,7% aller Verdächte wegen Betrug), Bern (15,4%), Genf (15,2%) und Tessin (12,1%); Bern (33,1% aller Verdächte wegen Missbrauch DVA), Zürich (31,2%), St. Gallen (16,4%) und Genf (5,9%). Betroffen sind somit bevölkerungsreiche Kantone und/oder solche mit einem wichtigen Finanzplatz. Beim Betrug lag sowohl der Wohnsitz des Vertragspartners (56,5% der Meldungen) sowie derjenige des wirtschaftlich Berechtigten (55%) mehrheitlich in der Schweiz; wichtige Herkunftsregionen waren zudem Westeuropa (Vertragspartner: 18,9%/wirtschaftlich Berechtigter: 24,8%), Zentralamerika und Karibik (12,3%/1,09%) sowie postsowjetische Staaten (2,1%/5,3%). Beim betrügerischen Missbrauch einer DVA wohnten sogar 90,5% der Vertragspartner und 89,7% der wirtschaftlich Berechtigten in der Schweiz. Zweite Herkunftsregion war Westeuropa (6%/6,4%). Die Tatsache, dass sehr viele Vertragspartner bzw. wirtschaftlich Berechtigte in der Schweiz wohnen, liegt wahrscheinlich daran, dass die Täter oft Finanzagenten[53] in der Schweiz anheuern und anschliessend diese Geschäftsbeziehungen der MROS gemeldet werden. Gegen Kommission stellen die Finanzagenten ihr Bankkonto zur Verfügung und leiten die eingehenden Summen anschliessend per Post oder Geldtransferinstitut an die Betrüger weiter. Die Identifizierung der Täter wird somit erheblich erschwert.

In über einem Drittel der gemeldeten Fälle (37,1%) zwischen 2016 und 2018 mit Betrug als mutmassliche Vortat war der Vertragspartner eine juristische Person. 40% davon waren Sitzgesellschaften, die übrigen 60% operativ tätige juristische Personen. Auch in diesem Bereich waren sowohl die juristischen Personen wie auch die wirtschaftlich Berechtigten primär in der Schweiz angesiedelt (beide 47%); häufig hatten juristische Personen als Vertragspartner zudem ihren Sitz in Zentralamerika und der Karibik (25,4%) sowie in Osteuropa (17,8%). Wirtschaftlich Berechtigte von juristischen Personen kamen ebenfalls oft aus Osteuropa (20%), aus den postsowjetischen Staaten (10,5%) und aus dem Nahen und Mittleren Osten (7,3%). Es ist anzunehmen, dass vor allem bei grossangelegten Betrugsmaschen auf aufwendige Firmenkonstrukte zurückgegriffen wird, um die Herkunft des unrechtmässig erlangten Geldes zu verschleiern.

Seit Juni 2015 wird zudem die Region, in der die Vortat stattfand, bei den Verdachtsmeldungen erfasst. Diese Daten sind besonders interessant, weil sie auch Informationen über Vortaten

[52] Seit 2015 sind allerdings – mit Ausnahme von 2016 – Korruptionsdelikte an erster Stelle; Betrug steht seitdem an zweiter Stelle.
[53] Die Finanzagenten werden auch Finanzmanager, Finanzintermediäre, Finanzrepräsentanten oder *Money Mules* genannt, cf. ebenfalls Unterkapitel 4.1.4.

geben, die im Ausland stattfanden und bei welchen der Schweizer Finanzplatz anschliessend für Geldwäschereizwecken missbraucht wurde. Die Daten (Juni 2015 bis Dezember 2018) zeigen aber, dass die Schweiz Hauptort für die Vortat bleibt: 44% der vermuteten Betrüge fanden hierzulande statt (Missbrauch einer DVA: 64%). Wichtigste Regionen im Ausland waren für den Betrug Westeuropa mit 22% (Missbrauch einer DVA: 14%), die postsowjetischen Staaten mit 9% (0,4%) und Nordamerika mit 3% (2%). In12% der Fälle beim Betrug (Missbrauch einer DVA: 18%) konnte die Vortat keiner Region zugeordnet werden.

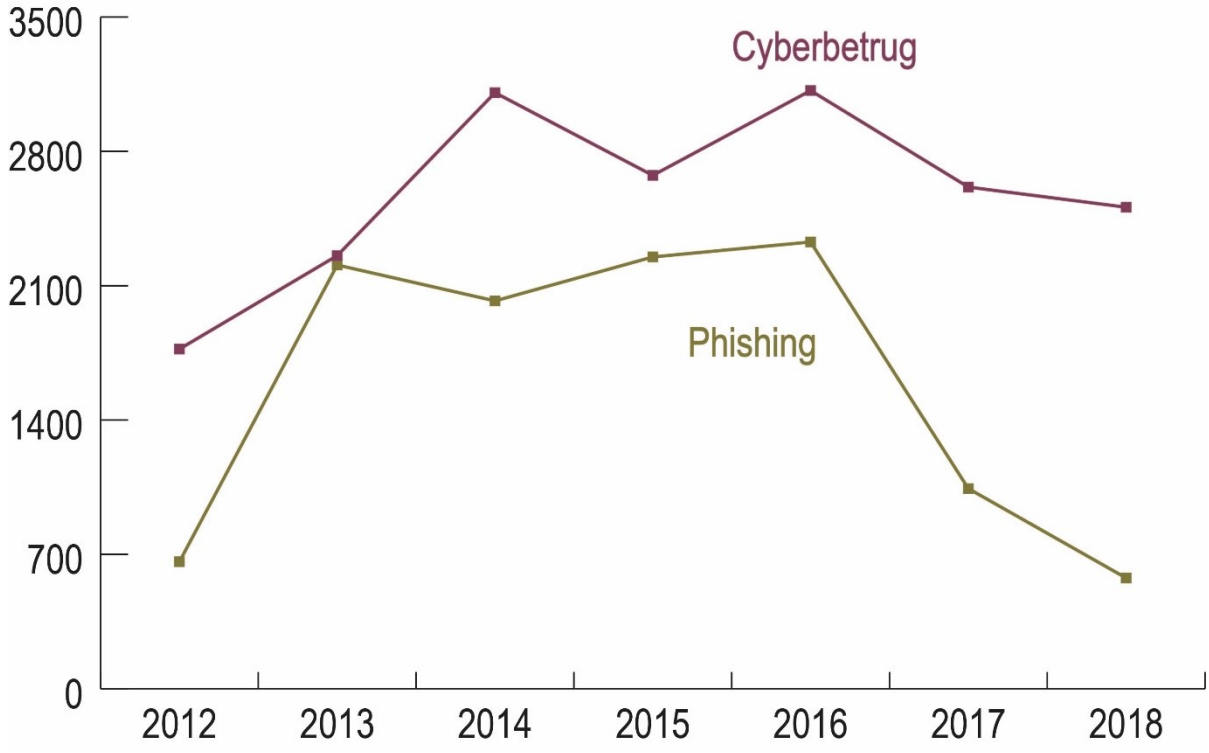
Die Finanzintermediäre meldeten hauptsächlich Verdachte basierend auf Informationen Dritter (Betrug: 35,9%/Missbrauch DVA: 84,6%). Es handelt sich dabei oft um Klagen von Geschädigten sowie um Swift-Nachrichten. Letztere erklären zumindest teilweise, warum die meisten Verdachtsmeldungen aus dem Bankensektor stammen. Beim Betrug dienten Zeitungsberichte (26,2%), Informationen von Strafverfolgungsbehörden (14,7%) und das eigene Transaktionsmonitoring (7,8%) ebenfalls als wichtige Meldungsauslöser.

Wie bei den Opferbefragungen sind die involvierten Summen auch bei der Mehrheit der Verdachtsmeldungen an MROS verhältnismässig tief. Sowohl beim Betrug (53%) als auch beim Missbrauch einer DVA (46%) ging es bei rund der Hälfte der Fälle um Summen unter 1’000 Franken. Insgesamt wiesen zwei Drittel (67%) der Meldungen beim Betrug und vier Fünftel (79%) der Meldungen beim Missbrauch einer DVA Schadensummen von höchstens 10'000 Franken auf. Beträge über eine Million Franken machten 7,7% aller Meldungen beim Betrug und 0,5% beim Missbrauch einer DVA aus. Höhere Summen kommen also eher beim Betrug als beim Missbrauch einer DVA vor, bleiben aber verhältnismässig selten.

Bei beiden Deliktarten hat die Meldung in rund der Hälfte der Fälle keine strafrechtlichen Konsequenzen (Meldung nach Analyse von MROS nicht weitergeleitet, Nichtanhandnahme, Nichteintreten, Verfahren sistiert oder eingestellt). Beim Betrug mündeten rund 4% aller Meldungen zwischen 2009 und 2018 in ein Urteil. Bei den restlichen Meldungen ist der Ausgang noch offen. Die Verurteilungsquote lag bei den Verdachtsmeldungen zum Missbrauch einer DVA mit 26,5% wesentlich höher als beim Betrug (Resultat noch offen: 26,5%). In der Regel wird aber bei letzterem Delikt der Finanzagent verurteilt und nicht der Haupttäter.

Zusammengefasst zeigt diese statistische Auswertung, dass vermutete Betrugsdelikte oft der Grund für eine Meldung an die MROS sind. Allerdings erweist sich in rund der Hälfte der Fälle der Verdacht als unbegründet, nicht nachweisbar oder allenfalls verjährt. Insbesondere bei Finanzagenten, die einen Grossteil der Meldungen ausmachen, ist der subjektive Tatbestand oft nicht erfüllt. Es ist zudem möglich, dass Betrug unter Umständen als eine Art Auffangtatbestand benutzt wird, wenn die Vortat nicht genau zuordenbar ist. Die festgestellte Zunahme der letzten Jahre deckt sich mit den Erkenntnissen aus der PKS. Es ist davon auszugehen, dass die gemeldeten Geschäftsbeziehungen vor allem Fälle mit Finanzagenten betreffen. Dafür sprechen auch die Tatsachen, dass die betroffenen Summen verhältnismässig tief sind und die meisten Vertragspartner und wirtschaftlich Berechtigten in der Schweiz wohnhaft sind. Bei mindestens einem Teil der Betrüge dürften Sitzgesellschaften im Ausland involviert worden sein, um die Herkunft der Gelder zu verschleiern. Auch wenn die meisten Vortaten in der Schweiz stattfanden, zeigen die Statistiken von MROS, dass vor allem beim Betrug die Straftat oftmals auch im Ausland verübt und die Gelder anschliessend hierzulande gewaschen werden.

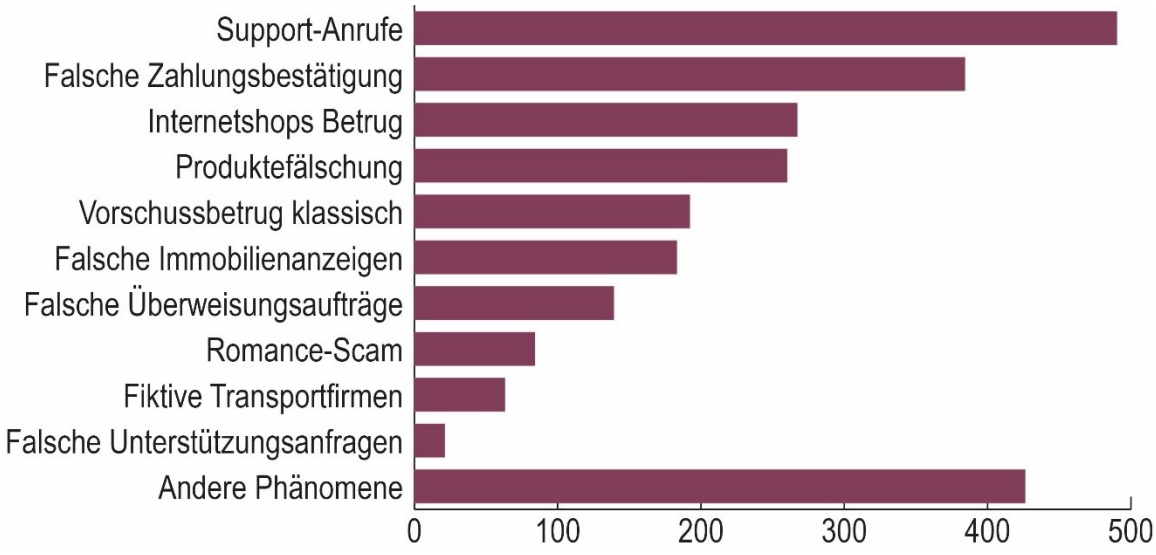
3.1.5 Verdachtsmeldungen zur Internetkriminalität an fedpol



Grafik 4: Verdachtsmeldungen zur Internetkriminalität an fedpol in den Jahren 2012-2018

Fedpol nimmt Verdachtsmeldungen aus der Bevölkerung zur Internetkriminalität entgegen (vgl. Kapitel 1.3), die per Onlineformular übermittelt werden. Ein Grossteil der Meldungen betrifft Strafbestimmungen von Schweizer Gesetzen. Die Anzahl Meldungen lässt aber keine gesicherten Schlüsse hinsichtlich des tatsächlichen Ausmasses der Internetkriminalität sowie der Zu- und Abnahme der illegalen Internetinhalte zu. Die Angaben widerspiegeln eher die Wahrnehmung der Gesellschaft von deliktischen Inhalten und Machenschaften im Bereich des Internets sowie die Bereitschaft, diese aktiv der Polizei und weiteren Behörden zu melden.[54] Bereits seit einigen Jahren gehen bei fedpol am häufigsten Meldungen zu Cyberbetrug und Phishing im weitesten Sinne ein. Hinweise zu diesen beiden Phänomenen machten in den vergangenen vier Jahren über die Hälfte aller Meldungen zur Internetkriminalität aus. Für das Jahr 2018 hat fedpol eine detaillierte Aufschlüsselung nach den spezifischen Betrugsphänomenen vorgenommen.

[54] Bundesamt für Polizei fedpol (2015): Jahresbericht der Nationalen Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIK 2014, S. 2. https://www.cybercrime.admin.ch/dam/data/kobik/Berichte/2015-03-26/jb-2015-d.pdf.



Grafik 5: Verdachtsmeldungen zur Internetkriminalität an fedpol im Jahr 2018

Die detaillierte Statistik veranschaulicht die grosse Bandbreite der verschiedenen Vorgehensweisen. Häufig gemeldet wurden 2018 insbesondere sogenannte Support-Anrufe (vorgegebene Hilfeleistung mit der Absicht der Täter, sich finanziell zu bereichern), falsche Zahlungsbestätigungen und Internetshop-Betrüge. Dabei werden immer wieder auch neue Modi Operandi beobachtet. Fedpol ist über neue Phänomene sehr rasch informiert und dient seinen Partnern dazu als Ansprechpartner.

3.1.6 Bewertung der allgemeinen Gefährdung

Opferbefragungen zeigen, dass Betrüge und Missbräuche einer DVA in der Schweiz weit verbreitet sind und dass nur ein Teil davon angezeigt wird. Bei sehr vielen Fällen bleibt es allerdings beim Versuch. Andere Fälle sind als geringfügige Vermögensdelikte einzustufen und bilden somit keine Vortat zur Geldwäscherei. Meistens liegen die Schadensummen pro Opfer im drei- bis vierstelligem Bereich; höhere Beträge kommen zwar vor, aber deutlich seltener. Nur 20% aller Verdachtsmeldungen an MROS mit vermuteter Vortat Betrug betreffen Summen über 10’000 Franken. Betrugsdelikte machen des Weiteren nur einen kleinen Teil aller Vermögensdelikte aus, die in der Schweiz begangen werden. Sie liegen zahlenmässig sowohl bei der PKS als auch bei der SUS weit hinter den Diebstahldelikten. Die Prävalenzraten in den Opferbefragungen liegen bei Diebstahldelikten ebenfalls um einiges höher als bei vollzogenen Betrugsstraftaten. Einige Statistiken, vor allem die PKS und die MROS-Meldungen, deuten auf eine tendenzielle Zunahme der Betrugsfälle in der Schweiz innerhalb der letzten Jahre hin. Vermutlich liegt dahinter eine teilweise Verlagerung der «klassischen» Eigentumsdelikten zur Internetkriminalität, wozu viele mithilfe des Internets durchgeführte Betrugsdelikte (Phishing, Vorschussbetrüge, usw.) gehören. Vor allem bei den Verdachtsmeldungen an MROS ist auch denkbar, dass die beobachtete Zunahme auf eine bessere Erkennung von Betrugsdelikten durch die Finanzintermediären zurückzuführen ist. Die aktuelle Faktenlage reicht allerdings nicht aus, um diese Hypothese bestätigen zu können.

Aus diesen Gründen ist für die Schweiz von einer höchstens mittleren potenziellen Geldwäschereigefährdung durch Betrug und betrügerischem Missbrauch von DVA auszugehen. Dies insbesondere angesichts der Tatsache, dass (i) Betrugsdelikte zwar häufig vorkommen, jedoch bei weitem nicht so oft wie andere Vermögensdelikte, dass (ii) die Schadensumme meistens im drei- bis vierstelligen Bereich liegt und dass (iii) nur vollzogene und nicht als geringfügig eingestufte Betrugsdelikte als Vortat zur Geldwäscherei fungieren können. Aufgrund der Heterogenität der Betrugsarten kann die potenzielle Gefährdung jedoch von Phänomen zu Phänomen anders ausfallen; dies wird in den nachfolgenden Unterkapiteln thematisiert.

Die konkrete Geldwäschereigefährdung kann nicht genau beziffert werden, da weder die PKS noch die SUS eine Analyse der Geldwäscherei nach der Vortat erlauben. Innerhalb der letzten

zehn Jahre (2009-2018) wurden 5'985 Meldungen mit Betrug als vermeintliche Vortat an MROS adressiert. Bislang wurden 255 Urteile gefällt (Missbrauch einer DVA: 1'116 Meldungen und 296 Urteile). Insgesamt werden in der Schweiz jährlich 180 bis 450 Urteile wegen Geldwäscherei gefällt. Viele haben entsprechend eine andere Vortat als ein Betrugsdelikt.[55] Zahlenmässig stellen die Betrugsdelikte in ihrer Gesamtheit also eine eher tiefe konkrete und juristisch bestätigte Geldwäschereigefährdung dar.

3.2 Gefährdung durch besondere Betrugsphänomene

Betrugsdelikte sind vielfältig. Es gibt keine abschliessende Auflistung von Betrugsarten, da Kriminelle immer neue Modi Operandi entwickeln.[56] Aufgrund der Analyse von Betrugsurteilen sowie öffentlichen und polizeiinternen Quellen konnten aber gewisse wiederkehrende Muster und Phänomene festgestellt werden, die nachfolgend präsentiert und hinsichtlich deren Gefährdung bewertet werden. Diese werden nach der von Levi (cf. Kapitel 2.1) angewandten Klassifizierung nach Opferkategorien eingeteilt. Wie bei jeder Klassifizierung handelt es sich um eine Vereinfachung der Realität zwecks besserer Übersicht. Die Codierung in Phänomene dient ebenfalls primär der Übersicht. In der Praxis können zudem verschiedene Modi Operandi im gleichen Fall kombiniert werden.

Es wurde versucht, sich an der – falls vorhanden – geläufigen Terminologie zu orientieren, die in der Schweiz für die jeweiligen Phänomene angewendet wird. Diese ist aber bei weitem nicht einheitlich und bezeichnet je nach Phänomen beispielsweise das Ziel des Betrugs (z.B. Kreditbetrug), den Geschädigten (z.B. Versicherungsbetrug) oder die Durchführungsart (z.B. Phishing). Gewisse Begriffe sind aber schon so stark eingebürgert, dass eine Umbenennung eher zu Verwirrung führen würde. Viele Betrugsdelikte greifen auf sogenanntes *Social-Engineering*-zurück. Darunter wird die gezielte Beeinflussung und Manipulation einer Person verstanden. Dabei wird zum Beispiel deren Hilfsbereitschaft oder Gutgläubigkeit ausgenutzt, mit dem Ziel an Daten zu gelangen oder die Person zu bestimmten Aktionen zu bewegen. Das Internet wird dabei als Tatmittel missbraucht (sogenannte *cyber-enabled crimes*).

3.2.1 Betrügerische Phänomene zulasten des öffentlichen Sektors

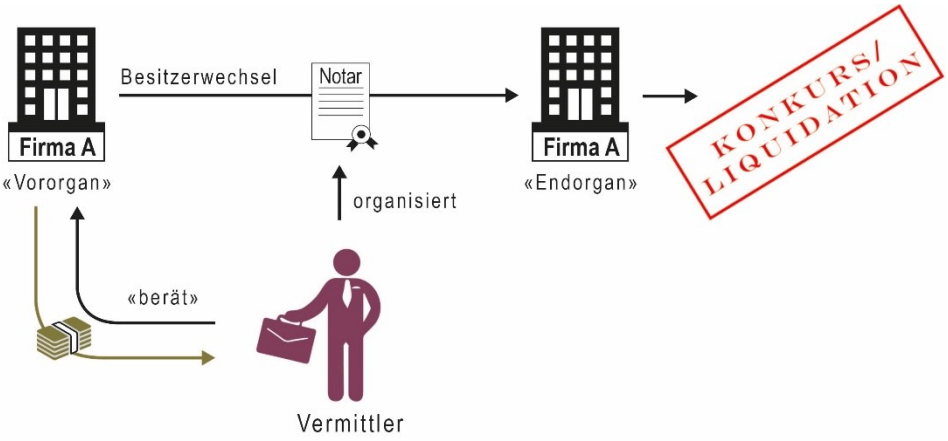
Straftaten mit Täuschungskomponenten zulasten des Staates sind oft von Sondertatbeständen erfasst, die nicht Gegenstand dieses Berichtes sind (s. Kapitel 2.4). Viele sind zudem als Vergehen oder als Übertretungen ausgestaltet und scheiden somit als Vortat zur Geldwäscherei aus, so zum Beispiel der Sozialhilfebetrug (148a StGB) oder der nicht qualifizierte Steuerbetrug. Das Staatsvermögen wird aber immer wieder von Betrügen im Sinne von Art. 146 StGB geschädigt; auch vereinzelt sind betrügerische Missbräuche einer Datenverarbeitungslage zulasten des öffentlichen Sektors denkbar. Nachfolgend aufgeführt sind einerseits Betrugsdelikte im Zusammenhang mit Firmenkonkursen, denn auch wenn in einem Konkurs meistens private Gläubiger involviert sind, gehört die öffentliche Hand oft zu den grössten Geschädigten. Andererseits sind weitere staatsbezogene Betrugsphänomene erwähnenswert, namentlich der Mehrwertsteuer-Karussellbetrug und der Betrug im Beschaffungswesen.

[55] Bei den letzten verfügbaren Daten aus der Periode 2008-2012 war die häufigste Vortat der Geldwäscherei Betäubungsmittelhandel (61% der Geldwäschereiurteile); Betrug kam mit 10% an zweiter Stelle. Bundesamt für Polizei fedpol (2014): Geldwäschereiurteile in der Schweiz. https://www.fedpol.admin.ch/dam/data/fedpol/publiservice/publikationen/berichte/geldwaeschereiurteile_okt2014-d.pdf.

[56] fedpol erstellt und aktualisiert laufend Faktenblätter zu Phänomenen im Bereich der Cyberkriminalität. Diese Faktenblätter sollen auch bei der Erkennung der infrage kommenden Straftaten helfen. Siehe Bundesamt für Polizei fedpol (2020): Betrugsarten.https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/cybercrime/gefahren/betrugsarten.html und Bundesamt für Polizei fedpol (2018): Gefahren im Internet. https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/cybercrime/gefahren.html.

a) *Betrugsdelikte im Zusammenhang mit Firmenkonkursen*

Straftaten im Zusammenhang mit dem Konkurs von Firmen betreffen üblicherweise die Tatbestände des betrügerischen Konkurses[57], der Gläubigerschädigung durch Vermögensverminderung[58] und der Misswirtschaft[59]. Je nach Konstellation kann aber auch ein Betrug im Sinne von Art. 146 StGB vorliegen, so bei der gewerbsmässigen Firmenbestattung. Bei diesem Modus Operandi wenden sich kleinere Firmen, die ihre Schulden nicht mehr begleichen können (sogenannte Vororgane), an einschlägig bekannte Vermittler, die gegen ein Beratungshonorar die Gesellschaften übernehmen und die notwendigen Formalitäten abwickeln. Die Vermittler versichern den Vororganen, dass sie sich auf diese Weise ihrer persönlichen Haftung entziehen und die überschuldete Gesellschaft gegen eine neue eintauschen können. Die Vororgane werden von den Vermittlern animiert, weitere Waren auf Rechnung zu bestellen oder Leasing-Verträge für Fahrzeuge abzuschliessen, die sie anschliessend ins Ausland verkaufen. Sobald die überschuldeten Firmen genügend ausgebeutet wurden, werden sie von einem sogenannten Endorgan übernommen. Endorgane werden von den Vermittlern eingesetzt und sind in der Regel vermögens- und erwerbslose Personen, die über keinerlei Erfahrungen in der Führung von Unternehmen verfügen. Ihre Hauptaufgabe besteht darin, eine möglichst grosse zeitliche, räumliche und inhaltliche Distanz zu den Vororganen zu schaffen, um deren Risiko zu vermindern, von den Gläubigern, den Konkursämtern oder den Strafverfolgungsbehörden in die Pflicht genommen zu werden.[60] Dafür werden sie von den Vermittlern mit einem Entgelt entschädigt. Nach einer gewissen Zeit werden die Gesellschaften liquidiert oder über sie wird der Konkurs eröffnet. Obwohl bereits bei Konkurseröffnung auffällt, dass das Endorgan auch mit anderen konkursiten Gesellschaften in Verbindung steht, ist das Ziel erreicht: Die Gesellschaft wird mangels Aktiven von Amtes wegen gelöscht und die Kosten werden abgeschrieben. Dadurch werden nicht nur private Gläubiger, sondern insbesondere die öffentliche Hand geschädigt[61]. Die Vor- und Endorgane machen sich in der Regel wegen verschiedener Konkursdelikte[62] und Betrug[63] strafbar. Gegen die Vermittler wird üblicherweise wegen Begünstigung, Betrug und Anstiftung zu Konkursdelikten ermittelt.



Grafik 6: Beispiel einer Firmenbestattung

Die Anzahl der eröffneten Firmen- und Privatkonkursverfahren nimmt in der Schweiz grundsätzlich seit 2000 zu (von 8'712 zu 15'291 Fälle im Jahr 2018). Der finanzielle Schaden aus

[57] Art. 163 StGB.
[58] Art. 164 StGB.
[59] Art. 165 StGB.
[60] Sakic, Senad (2015): Gewerbsmässige Firmenbestattung. Masterarbeit am Competence Center Forensik und Wirtschaftskriminalität. Hochschule Luzern. 2015, S. 6.
[61] Ibd., S. 15.
[62] Betrügerischer Konkurs und Pfändungsbetrug (Art. 163 StGB), Gläubigerschädigung durch Vermögensminderung (Art. 164 StGB), Misswirtschaft (Art. 165 StGB), Unterlassung der Buchführung (Art. 166 StGB).
[63] Bestell- und Leasingbetrug (Art. 146 StGB).

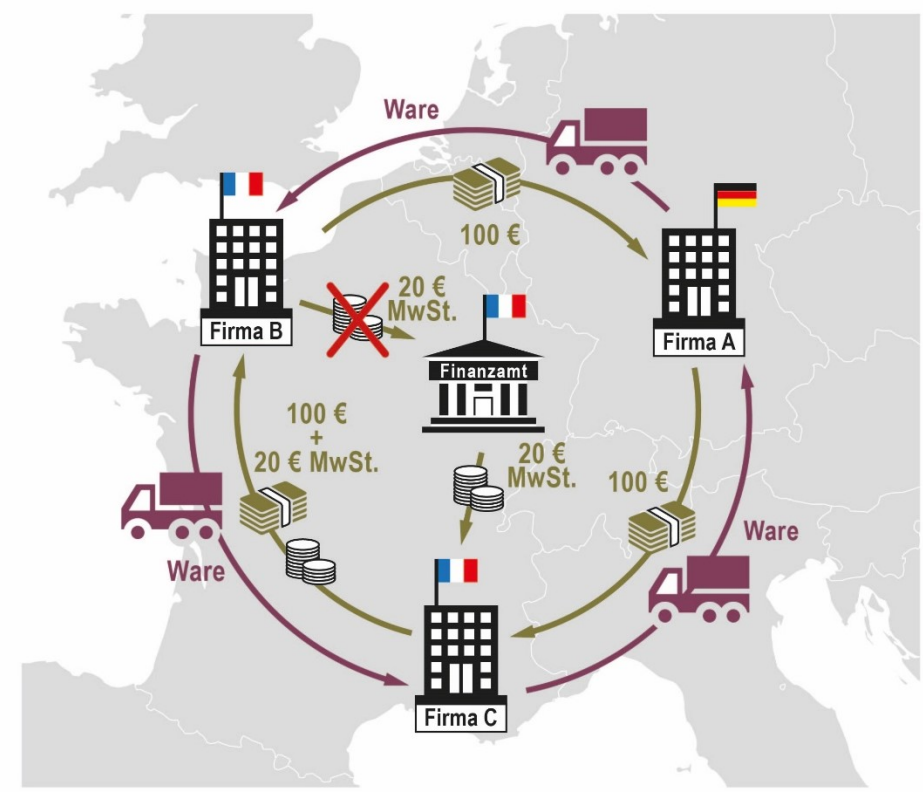
ordentlichen und summarischen Konkursverfahren betrug 2018 rund 2 Milliarden Franken.[64] Wie viel davon auf betrügerische Handlungen zurückzuführen ist, lässt sich nur grob abschätzen. 2016 gingen die Zürcher Behörden in ihrem Kanton von einem jährlichen Schaden von über 200 Millionen Franken aus, welcher durch Firmenbestattungen entstehen würde.[65] Hochgerechnet auf die ganze Schweiz würde dies einem jährlichen Schaden von über einer Milliarde Franken entsprechen.

Die Zahlen in der PKS und SUS sind weit bescheidener, sprechen aber für eine tendenzielle Zunahme des Phänomens. So hat sich beispielsweise die Anzahl Verurteilungen wegen Misswirtschaft zwischen 2008 und 2018 von 41 auf 237 mehr als verfünffacht. Beim betrügerischen Konkurs ist die Entwicklung nicht so ausgeprägt, tendiert aber mit 240 Verurteilungen im Jahr 2018 (2008: 115) in die gleiche Richtung. Es ist von einem erheblichen Dunkelfeld auszugehen. Wie viele der Gelder anschliessend gewaschen werden, lässt sich anhand der aktuellen Sachlage nicht einschätzen. Wie bereits erwähnt, bilden betrügerische Konkurse zudem nicht in jedem Fall eine Vortat zur Geldwäscherei.

b) *Mehrwertsteuer–Karussellbetrug*

Bei einem Mehrwertsteuer-Karussellbetrug geht es hauptsächlich darum, einer Firma den Vorsteuerabzug für eine nie abgelieferte Mehrwertsteuer zu ermöglichen. Vereinfacht dargestellt spielt sich dieser Modus Operandi wie folgt ab (vgl. Grafik): Das Unternehmen B mit Sitz in einem europäischen Land (Frankreich) gibt vor, Waren oder Dienstleistungen im Wert von 100 Euro von dem Unternehmen A mit Sitz in einem anderen europäischen Land (Deutschland) zu kaufen. Diese Transaktion entspricht einer sogenannten innergemeinschaftlichen Lieferung und ist daher gemäss EU-Mehrwertsteuergesetzgebung steuerbefreit. B liefert diese meist fiktiven Waren oder Dienstleistungen anschliessend an das Unternehmen C, das seinen Sitz im selben Land wie B hat. Diese zweite Stufe des Karussells ist nicht mehr steuerbefreit, daher verrechnet B dem Unternehmen C den Preis der Waren plus die anfallende Mehrwertsteuer (100 Euro plus 20 Euro Mehrwertsteuer). Da der ganze Handel nur fiktiv ist, fliesst in Wahrheit meist kein Geld. B müsste nun die Mehrwertsteuer ans Finanzamt weiterleiten, kommt dieser Verpflichtung aber nicht nach. B wird in diesem System *Missing Trader* genannt, weil die Firma verschwindet, sobald das Karussell auffliegt. Meist handelt es sich dabei um Briefkastenfirmen, die von Strohmännern geführt werden. C verkauft die Waren nun wieder an A. Dieser Vorgang entspricht wieder einer innergemeinschaftlichen Lieferung und ist daher für C und A steuerneutral. C kann aber die zuvor an B entrichtete Mehrwertsteuer als Vorsteuerabzug geltend machen und bekommt die 20 Euro dadurch vom Finanzamt «zurück»-erstattet. Gesamthaft gesehen haben sich die Betrüger somit die Mehrwertsteuer «zurück»-erstatten lassen, ohne sie jemals bezahlt zu haben. Nun verkauft A die Waren wieder an B und das Karussell beginnt sich von neuem zu drehen. In den meisten Fällen werden vor allem zwischen B und C noch weitere Unternehmen zwischengeschaltet, um die Komplizenschaft der beiden Firmen zu verschleiern und die Ermittlungen zu erschweren. Diesen sogenannten *Buffern* ist oftmals gar nicht bewusst, dass sie für einen Karussellbetrug benutzt werden.

[64] Cf. Bundesamt für Statistik (2019c): Zahl der Konkurseröffnungen steigt erneut an. Version vom 11.04.2019. https://www.bfs.admin.ch/bfsstatic/dam/assets/7966844/master.
[65] SRF (2016): Konkursreiterei: Mehrere Hundert Millionen Schaden im Jahr. 13.04.2016. https://www.srf.ch/news/schweiz/konkursreiterei-mehrere-hundert-millionen-schaden-im-jahr.



Grafik 7: Schematische Darstellung einer Mehrwertsteuer-Karussellbetrug

Gemäss Entscheid des Bundesgerichts[66] ist ein Karussellbetrug in der Schweiz als Betrug im Sinne von Art. 146 StGB zu werten und nicht etwa als Abgabebetrug. Der Karussellbetrug gilt somit schon lange als Vortat zur Geldwäscherei. Die Täter sind hauptsächlich gut organisierte, europäische Gruppierungen, die mehrheitlich aus vorbestraften Betrügern bestehen. Im Zuge der EU-Erweiterung konnten vermehrt osteuropäische Drahtzieher von Mehrwertsteuer-karussells enttarnt werden.

Zuverlässige Zahlen zum Umfang von Mehrwertsteuer-Karussellbetrügen in der Schweiz existieren nicht. Wegen dem im Vergleich zum europäischen Durchschnitt niedrigen Mehrwertsteuersatz ist der Schweizer Fiskus nur sehr selten die geschädigte Partei. Es kann jedoch vorkommen, dass sich ein *Buffer* in der Schweiz befindet. Beim Mehrwertsteuer-Karussellbetrug handelt sich um ein typisches Beispiel für Delikte, bei welchen die Vortat sich meistens im Ausland abspielt und der Schweizer Finanzplatz anschliessend zu Geldwäschereizwecken missbraucht wird.

c) *Betrug im Beschaffungswesen*

Bei einem Betrug im Beschaffungswesen wird ein öffentlicher Auftrag einem Privaten auf Basis einer arglistigen Täuschung vergeben. Der Betrugstatbestand steht somit vor allem dann im Vordergrund, wenn das strafbare Verhalten aufseiten des Anbietenden liegt.[67] Aber auch ein Verwaltungsangestellter kann sich des Betrugs schuldig machen, etwa wenn er seinen Vorgesetzten über die Rechtmässigkeit des zu bewilligenden Auftrages täuscht (siehe Fallbeispiel). Ungeklärt ist die Frage, ob ein Submissionskartell auch ein Betrug im Sinne von Art. 146 StGB darstellen kann.[68]

---

[66] Urteil (des Bundesgerichts) 1A.189/2001 vom 22.2.2002.
[67] Galli, Peter et al. (2013): Praxis des öffentlichen Beschaffungsrechts. Eine systematische Darstellung der Rechtsprechung des Bundes und der Kantone. 3. Auflage. Zürich 2013, S. 551.
[68] Vgl. Ackermann, Jürg-Beat (2019): Das Submissionskartell – Sicht des Strafrechts. Luzern 18.02.2019. https://www.unilu.ch/fileadmin/fakultaeten/rf/diebold/Tagung_Submissionskartell/Ackermann_Submissionskartell_Strafrecht.pdf; Galli et al., op. cit., S. 551-552.

Missbräuche im Beschaffungswesen der Eidgenossenschaft, der Kantone und Gemeinden sind vermutlich weit verbreiteter als es die vergleichsweise seltenen Strafverfahren in diesem Bereich nahelegen. Auch im Ausland sind strafbare Unregelmässigkeiten bei Kaufhandlungen des Staates keine Seltenheit. Oft werden diese Taten mit den Strafbestimmungen, die die Amts- und Berufspflichten regeln, oder mit dem Korruptionsstrafrecht geahndet. Betrüge im Sinne von Art. 146 StGB kommen aber auch wiederholt vor, eine genau Einschätzung ist aufgrund der lückenhaften Faktenlage jedoch nicht möglich.

Fallbeispiel Betrug im Beschaffungswesen
A arbeitete jahrelang als Projektleiter bei einem Staatsbetrieb. Zwischen 2002 und 2014 vergab er unrechtmässig freihändige Aufträge an drei Firmen für einen Gesamtwert von über 11 Millionen Franken. Ein wesentlicher Teil der verrechneten Leistungen wurden nicht oder nur zum Teil ausgeführt. A verfasste selber viele Offerten für Aufträge, die er danach auch vergab. Er musste auch die, nach den angeblich erbrachten Leistungen, gestellten Rechnungen überprüfen und diese seinem Linienvorgesetzten zur Freigabe weiterleiten. Dabei nutzte A das Vertrauensverhältnis mit seinem Vorgesetzten und die Tatsache aus, dass jener nicht in der Lage war, die materielle Korrektheit der Rechnungen zu prüfen. Ein grosser Teil des auf 600'000 Franken geschätzten Verbrechenserlöses gab A für seinen Lebensunterhalt und denjenigen seiner Familie, für Restaurantbesuche und Ferien aus. Aus diesen Gründen wurde A im Juni 2018 vom Bundestrafgericht wegen gewerbsmässigen Betrugs und einfacher Geldwäscherei sowie wegen ungetreuer Amtsführung, Sich-bestechen-Lassens und Vorteilsannahme zu einer teilbedingten Freiheitstrafe von 36 Monaten und einer bedingten Geldstrafe von 150 Tagesätzen verurteilt.

3.2.2 Betrügerische Phänomene zulasten von Unternehmen

Unternehmen stellen interessante Ziele für Betrüger dar, da sie dort potenziell hohe Summen entwenden können. Kleine und mittlere Unternehmen (KMU), die das Rückgrat der Schweizer Wirtschaft bilden, sind besonders gefährdet, da diese nicht immer über die nötigen Ressourcen und das nötige Knowhow verfügen, um sich gegen Betrugsmaschen effizient zu schützen. Aber auch grosse Firmen können betrogen werden. Häufige Phänomene sind falsche internationale Überweisungsaufträge, Phishing sowie Kredit- und Versicherungsbetrüge. Konkursbetrüge, die oft auf Unternehmen als Geschädigten haben, wurden schon oben abgehandelt.

a) *Phishing*

Phishing (Kofferwort aus Passwort, *Harvesting* und *Fishing*) bezeichnet den Vorgang, bei dem versucht wird, einem Benutzer durch Irreführung und auf unbefugte Weise vertrauliche Daten zu entlocken. Zu diesem Zweck verschicken die Täter beispielsweise E-Mails, in welchen das Opfer aufgefordert wird, seine persönlichen Daten für E-Mail-Konten, Kreditkarten oder E-Banking-Systeme zu aktualisieren. Der Versand von Phishing-Mails erfolgt häufig über Botnetze. Phishing-Seiten sind meistens im Ausland gehostet und können sich auf gehackten Servern von Drittparteien befinden. Die gestohlenen Daten können weiterverkauft und von einer anderen Täterschaft wiederverwendet werden. In der Regel ist der Versand von Phishing-Mails nicht strafbar. Je nach Ausgestaltung der gefälschten Internetseiten bzw. der gefälschten E-Mails ist möglicherweise der Straftatbestand der Urkundenfälschung erfüllt.[69] Benutzt der Täter die erhaltenen Daten, um Vermögenswerte zum Nachteil des Geschädigten zu verschieben, ist der Straftatbestand des betrügerischen Missbrauchs einer Datenverarbeitungsanlage im Sinne von Art. 147 StGB anwendbar. Beim Staat oder bei Unternehmen kann Phishing auch dazu dienen, verbotene nachrichtendienstliche Tätigkeiten auszuüben (Art. 272-274 StGB). Da die Banken ihre Sicherheitsmassnahmen in den letzten Jahren kontinuierlich verbessert haben, greifen kriminelle Gruppierungen seit Ende 2006 vermehrt auf den Einsatz von Malware zurück, welche die DNS-Einstellungen derart ändern können, dass das Opfer unbemerkt auf eine gefälschte Webseite geleitet wird und dort die vertraulichen Informationen eingibt (*Pharming*). Wenn es den Tätern gelingt, Gelder unrechtmässig zu verschieben, erfüllt ihre

[69] Vgl. BGE 116 IV 343.

Handlung auch hier den Tatbestand des betrügerischen Missbrauchs einer Datenverarbeitungsanlage.[70] Um die Spur der betrügerisch erlangten Gelder zu verschleiern, setzen die Betrüger grösstenteils Finanzagenten ein, die gegen Kommission ihr Konto für die deliktischen Zahlungen zur Verfügung stellen. Sobald das Geld auf dem Konto eines Finanzagenten eingegangen ist, wird dieser angewiesen, die Summe bar zu beziehen und via Geldüberweisungsinstitut oder per Post an einen unbekannten Empfänger zu überweisen.

Der genaue Umfang von Phishing ist schwer einzuschätzen, da viele Versuche automatisch von Spamfiltern und anderen Schutzmechanismen aussortiert werden. In einer von PwC 2017 durchgeführten Umfrage zur Wirtschaftskriminalität war Phishing die häufigste angewendete Technik gegen Unternehmen im Bereich Cyberkriminalität.[71] Auch Privatpersonen sind vom Phänomen stark betroffen. Hochrechnungen in der Studie von Beaudet-Labrecque et al. ergaben 2018, dass in der Schweiz über eine halbe Millionen Personen ab 55 Jahre innerhalb der letzten fünf Jahre mit einem Versuch von Phishing konfrontiert war (entspricht einer Prävalenz von rund 20%).[72] Bei jüngeren Generationen dürften vermutlich fast alle mindestens einmal mit einem Phishingversuch konfrontiert worden sein. Die 577 Internetverdachtsmeldungen bezüglich Phishingfällen, die fedpol 2018 online übermittelt wurden, dürften somit die aktuelle Lage nur bruchstückhaft widerspiegeln. Mit einem erfolgreichen Phishingversuch liegt erst eine vorgelagerte Handlung zur allfälligen Geldwäscherei vor, da soweit noch kein finanzieller Schaden entstanden ist.

b) *Falsche internationale Überweisungsaufträge (FOVI)*

Der ursprünglich als CEO-Betrug bekannte Modus Operandi hat sich in verschiedene Varianten weiterentwickelt, die je nach Land oder Behörde unter anderem als «falsche internationale Überweisungsaufträge» (FOVI – *escroquerie aux faux ordres de virement internationaux*), *Social Engineering* oder *Business E-mail Compromise Fraud* (BEC) bezeichnet werden.[73] Folgende Varianten kommen immer wieder vor:

- Beim *CEO-Betrug* (im engeren Sinne) geben sich die Täter als Geschäftsführer oder Finanzverantwortliche des von ihnen kontaktierten Unternehmens aus. Mit vielen Techniken versuchen sie, die Mitarbeiter dazu zu bewegen, eine oder mehrere Bankzahlungen zu ihren Gunsten auszulösen. Alternativ versuchen die Täter, die E-Mail-Kontos von Mitarbeitern zu hacken oder ähnlich klingende Adressen vorzutäuschen, um von diesen Adressen aus Zahlungsbefehle an die Finanzdienste zu erteilen.
- Beim *Betrug mit falschen Banktechnikern* zielen die Täter ebenfalls auf private Unternehmen. Sie geben sich per Telefon als Angestellte einer Bank aus und verschaffen sich mit verschiedenen Tricks Zugang zur E-Banking-Session der Geschädigten. Sie lösen anschliessend mehrere Überweisungen zu ihren Gunsten aus. Alternativ versuchen die Täter, sich als Geschäftspartner auszugeben (z.B. Anwalt, Immobilienmakler, Lieferanten, usw.) und weisen die Mitarbeiter der Firma hin, künftig die Zahlungen auf ein anderes, von den Kriminellen kontrolliertes Konto zu überweisen.
- Beim *Betrug mit falschem Immobilienmakler* versuchen die Täter, die bestehenden Zahlungsbefehle einer Immobilienverwaltung oder eines Immobilienmaklers durch verschiedene Techniken zu ändern. Dabei geben sie sich als Immobilienmakler oder als in solche Transaktionen involvierte Personen aus und weisen die Opfer an, das Geld auf ein von ihnen kontrolliertes Konto zu überweisen.

Solche Betrüge erfordern eine minutiöse, teilweise monatelange Vorbereitung, um glaubhaft zu wirken. Die Betrüger sammeln im Vorfeld alle verfügbaren Informationen über die Firma, deren Organigramm, Zahlungsmodalitäten, Bankverbindungen, Geschäftsfelder, laufende

[70] Bundesamt für Polizei fedpol (2011b): Finanzagenten – Geldwäscherei als lukrative Nebenbeschäftigung (intern), S. 2.
[71] PricewaterhouseCoopers PwC (2018), op. cit. S. 10.
[72] Beaudet-Labrecque et al. (2018b), op. cit.
[73] Cf. Egmont Group of Financial Intelligence Units (2019): *Business Email Compromise Fraud*, in: Egmont Group Bulletin, S. 3-4. https://www.egmontgroup.org/sites/default/files/filedepot/external/20190708_EGMONT%20GROUP%20BEC%20BULLETIN-final.pdf.

Projekte, Partnerschaften etc. und schrecken auch nicht davor zurück, E-Mail-Konten von Angestellten zu hacken. Die ausgewählten Mitarbeiter aus der Finanzabteilung werden telefonisch oder per E-Mail aufgefordert, beispielsweise im Zusammenhang mit einer noch streng geheimen Übernahme eines anderen Unternehmens, sofort eine grössere Zahlung zu veranlassen. Nicht selten setzen sie sich zudem vorgängig mit der Bank in Verbindung und geben eine Änderung der Telefonnummer bekannt. Falls der verantwortliche Bankangestellte Zweifel an der Legitimität der Überweisung hat und diese überprüfen möchte, wird ihm der Betrüger am anderen Ende der Leitung den Auftrag bestätigen. Teilweise kontaktieren die Betrüger auch direkt den Kundenberater oder Treuhänder und geben sich als Direktor der Firma aus. Dabei verwenden sie das Logo des Unternehmens und eine Mailadresse, die derjenigen des Direktors sehr ähnlich ist. In der Regel operieren die Täter vom Ausland aus, typischerweise im Nahen Osten, wo die Vermögenswerte, oft nach einem Umweg über ein asiatisches Land, auch regelmässig landen. Betroffen vom Betrug sind sowohl KMU als auch grössere Unternehmen aller Wirtschaftssektoren.

Gesamtzahlen zum Umfang der falschen internationalen Überweisungsaufträge in der Schweiz existieren nicht. Zwischen 2015 und 2018 betrafen 3,8% der klassifizierten Verdachtsmeldungen an fedpol zur Internetkriminalität dieses Phänomen. In dieser Zeitspanne schwankte die Anzahl Meldungen zwischen 95 (2015) und 210 (2017). Bei der Variante CEO-Betrug hat fedpol Kenntnis von mindestens 238 Fällen, die zwischen 2010 und 2017 stattfanden, wovon 59 aus Sicht der Täter erfolgreich waren. Der unmittelbare Gesamtschaden betrug über 34 Millionen Franken. In der Schweiz, aber auch in verschieden anderen Ländern gehen die Zahlen von gemeldeten CEO-Betrügen tendenziell zurück; die Täter scheinen mittlerweile andere Varianten des Phänomens zu bevorzugen.

Falsche Überweisungsaufträge dürften als Phänomen deutlich seltener vorkommen als beispielsweise der Vorschussbetrug; vollzogene Fälle dürften in der Schweiz jährlich im dreistelligen Bereich liegen. Allerdings erreicht der Schaden pro erfolgreichem Betrug oft einige hunderttausend Franken. Im schlimmsten Fall kann es zum Konkurs der Firma kommen. Da die meisten Fälle internationale Geldtransfers erfordern, die oft wenig kooperative Staaten involvieren, dürfte bei vielen der vollzogenen Fälle eine Geldwäschereihandlung vorliegen.

c) *Kreditbetrug*

Bei einem Kreditbetrug versuchen die Täter mithilfe von wahrheitswidrigen Angaben zu Einkommensverhältnissen, Bonität, Zahlungsabsicht oder anderen Kriterien einen Kredit zu erlangen. Dabei haben sie keine Absicht, diesen Kredit jemals zurückzubezahlen. In den meisten Fällen greifen sie für den Kreditantrag auch auf gefälschte Dokumente zurück. Ein solches Verhalten wird durch den Straftatbestand des Betrugs aufgefangen. Ein spezifischer Tatbestand des Kreditbetrugs existiert in der Schweiz nicht. In der Vergangenheit wurden sowohl Einzeltäter als auch organisierte Gruppierungen wegen Betrug nach diesem Modus Operandi verurteilt. Häufig wurden die Täter auch der Geldwäscherei schuldig gesprochen, da sie die erschlichenen Kredite bar bezogen, weitertransferiert oder ausgegeben hatten.

Zuverlässige Zahlen zum Umfang des Phänomens liegen fedpol nicht vor. Die jährliche Anzahl Kreditbetrüge dürfte im dreistelligen Bereich liegen. Es ist davon auszugehen, dass die Täter das betrügerisch erlangte Geld nicht nur auf ihren eigenen Konten horten werden. Daher dürfte meistens eine Geldwäschereihandlung vorliegen (Gegenbeispiel: cf. Kasten unten).

Fallbeispiel Kreditbetrug
Im Kanton Aargau wurden 2015 zwei Personen aus einem südosteuropäischen Land wegen gewerbsmässigen Betrugs und Urkundenfälschung verurteilt. Es handelte sich dabei um eine grosse Betrugsserie mit insgesamt rund 270 angezeigten Delikten und einer Deliktsumme von knapp 3,5 Millionen Franken. Der Fall kam durch eine Geldwäscherei-Meldung der betroffenen Bank ins Rollen. Neben den Tätern im Kanton Aargau war in Bern eine weitere Zelle mit drei Haupttätern mit dem gleichen Modus Operandi tätig. Die Täter gingen immer nach demselben Schema vor: Sie beantragten bei der gleichen Schweizer Bank mittels Online-Kreditantrag einen Privatkredit im Umfang von 25'000 bis 80'000 Franken auf die Namen von Mittätern. In den Kreditanträgen machten sie wahrheitswidrige Angaben zu den Einkommensverhältnissen und über die Bonität der Kreditnehmer und reichten dazu gefälschte Lohnabrechnungen und Betreibungsregisterauszüge ein. Teilweise gaben die Täter auch ein falsches Geburtsdatum an und übermittelten der Bank gefälschte Ausweise, damit die vorgeschobenen Kreditnehmer bei Datenbankabfragen mittels Geburtsdatum nicht auffindbar waren. Sobald die Kredite genehmigt und ausbezahlt wurden, bezogen die Täter die Summen in bar. Aufgrund sich häufender Betrugsversuche nahm die Bank eine vertiefte Kontrolle der eingereichten Dokumente vor und es kam daraufhin bei mehreren der angezeigten Delikte nicht zur Auszahlung des Kredits. In der Anklageschrift beantragte die Staatsanwaltschaft gegen einen Täter auch einen Schuldspruch wegen Geldwäscherei. Sie machte geltend, dass er den auf den Namen seines Bruders beantragten Kredit im Umfang von 74'000 Franken mittels Kontovollmacht in bar bezogen und einen Teil davon anschliessend auf ein auf seinen eigenen Namen lautendes Konto bei einer anderen Bank einbezahlt hatte. Die gesamte Summe verbrauchte der Beschuldigte für persönliche Zwecke. Das Gericht sprach den Beschuldigten jedoch vom Vorwurf der Geldwäscherei frei. Der Beschuldigte wurde zu einer Freiheitsstrafe von drei Jahren verurteilt, wovon ihm für 24 Monate der bedingte Strafvollzug gewährt wurde. Die geschädigte Bank hat gegenüber dem Beschuldigten zudem Zivilforderungen angemeldet.

d) *Versicherungsbetrug*

Mit dem Versicherungsbetrug erwirken die Täter die Auszahlung einer Versicherungssumme unter falschen Voraussetzungen. Solche Betrüge können sowohl zulasten von Privatversicherungsunternehmen als auch staatlichen Behörden begangen werden. Handeln die Täter nicht arglistig werden sie nach Art. 148a StGB, der einen unrechtmässigen Bezug von Leistungen einer Sozialversicherung oder der Sozialhilfe mit Freiheitsstrafe bis zu einem Jahr bedroht, geahndet. Zudem sehen verschiedene Gesetze im Bereich des Bundessozialversicherungsrecht sowie kantonale Erlasse (z.B. kantonale Sozialhilfeerlasse) eigene Strafbestimmungen vor.[74] All diese Straftaten stellen als Vergehen oder Übertretungen jedoch keine Vortat zur Geldwäscherei dar. Arglistig durchgeführte Täuschungen von Versicherungen können aber unter die Voraussetzungen von Betrug im Sinne von Art. 146 StGB fallen; sie können von Versicherten wie auch von einem Leistungserbringer (z.B. ein Arzt, der an die Patientenversicherung Rechnungen schickt für fiktive oder überhöhte Leistungen) begangen werden. Je nach Konstellation fällt der Betrugstatbestand aufgrund mangelnder Stoffgleichheit aus (cf. Unterkapitel 4.2). Wenn ein Leasingnehmer sein Leasingfahrzeug mit Vollkaskoversicherung als

[74] Vgl. Art. 87 des Bundesgesetzes über die Alters- und Hinterlassenenversicherung (AHVG) vom 20. Dezember 1946 (SR 831.0); Art. 76 des Bundesgesetzes über die berufliche Alters- , Hinterlassenen- und Invalidenvorsorge (BVG) vom 25. Juni 1982 (SR 831.40); Art. 92 des Bundesgesetzes über die Krankenversicherung (KVG) vom 18. März 1994 (SR 832.0); Art. 31 des Bundesgesetzes über Ergänzungsleistungen zur Alters-, Hinterlassenen- und Invalidenversicherung (ELG) vom 6. Oktober 2006 (SR 831.30); Art. 105 des Bundesgesetzes über die obligatorische Arbeitslosenversicherung und die Insolvenzentschädigung (AVIG) vom 25. Juni 1982 (SR 837); Art. 23 des Bundesgesetzes über die Familienzulagen (FamZG) vom 24. März 2006 (SR 836.2) in Verbindung mit Art. 87 AHVG; Art. 25 des Bundesgesetzes über den Erwerbsersatz für Dienstleistende und bei Mutterschaft (EOG) vom 25. September 1952 (SR 834.1) in Verbindung mit Art. 87 AHVG; Art. 70 des Bundesgesetzes über die Invalidenversicherung (IVG) vom 19. Juni 1959 (SR 831.20) in Verbindung mit Art. 87 AHVG.

gestohlen meldet, um sich von der Bezahlung der Raten zu befreien, begeht er keinen Versicherungsbetrug, sondern allenfalls eine arglistige Vermögensschädigung im Sinne vom Art. 151 StGB.[75]

Bei einer 2017 durchgeführten Studie im Auftrag des Schweizerischen Versicherungsverbands gaben fast zehn Prozent der Befragten zu, dass sie oder ein anderes Mitglied aus deren Haushalt schon einmal nicht existierende oder übertriebene Kosten bei einer Versicherung geltend gemacht haben.[76] Am meisten geschummelt wurde mit den Hausrat- und Privathaftpflichtversicherungen. Viele dieser Fälle dürften allerdings entweder als unrechtmässigen Bezug von Versicherungsleistungen im Sinne von Art. 148a StGB oder als geringfügige Betrugsdelikte gelten, sodass eine Geldwäschereistraftat von vornherein ausgeschlossen ist.

e) *Lebensmittelbetrug*

Betrügerische Praktiken mit Lebensmitteln sorgen immer wieder für Schlagzeilen. Betrüge reichen vom lokalen Restaurantbetreiber, der seinen Kunden Pferde- als Rindfleisch serviert, bis hin zu Lebensmittelbetrug im grossen Stil begangen durch kriminelle Organisationen.[77] Dabei handelt es sich um betrügerische Praktiken in der Lebensmittelkette, unter anderem, den Verkauf von minderwertigen, gefälschten und falschen Lebensmitteln.

Stichprobenartige Kontrollen lassen auf eine erhebliche Dunkelziffer schliessen. Aufgrund des Kausalzusammenhangs und der Stoffgleichheit sind vor allem bei grossen Lebensmittelbetrügen mit komplizierten Lieferketten rechtlich gesehen oft intermediäre Unternehmen (in der Regel Grosshändler oder Einzelhandel) die Geschädigten und nicht der Endkunde. Sind die Tatbestandsmerkmale des Betrugs nicht erfüllt – unter anderem der Tatbestand der Arglist – werden betrügerische Praktiken je nach Fallkonstellation als Täuschung im Sinne von Art. 64 des Lebensmittelgesetzes (LMG)[78] geahndet oder als Warenfälschung nach Art. 155 StGB.[79] Die Täuschung im Sinne des LMG ist eine Übertretung und die nicht qualifizierte Warenfälschung ein Vergehen; beide bilden somit keine Vortat zur Geldwäscherei.[80]

Um den Lebensmittelbetrug zu bekämpfen, koordinieren seit 2011 Europol und Interpol die sogenannten OPSON-Operationen. Die Schweiz nahm seit 2017 an drei dieser Operationen teil (OPSON VI, OPSON VII und OPSON VIII). Untersucht wurden Bio-Getreide aus Osteuropa (OSPON VI in Kombination mit nationaler Kontrollkampagne), das «Schönfärben» von Thunfisch (OPSON VII) und die Kaffee-Kennzeichnungen (OPSON VIII). Bei 4 (Thunfischfärbung)

---

[75] Maeder, Stefan/ Niggli, Marcel Alexander (2019): *Art. 146*, in: Niggli, Marcel Alexander / Wiprächtiger, Hans (Hrsg.): Strafrecht II, Art. 111–392 StGB. Basler Kommentar, 2. Aufl., Basel 2019, S. 3053; BGE 134 IV 210.
[76] SVV (2017): Versicherungsbetrug: Zahlen und Fakten. Zusammenfassung der Ergebnisse der GfK Studie zum Versicherungsmissbrauch. 31.08.2017, S. 5 https://www.svv.ch/sites/default/files/2017-11/SVV%20Zusammenfassung%20der%20Ergebnisse%20der%20GfK%20Studie%20zum%20Versicherungsmissbrauch%202017.pdf.
[77] Vgl. zum Beispiel: NTV (2012): Handel mit Falsch-Käse entlarvt. 17.06.2012. https://www.n-tv.de/panorama/Handel-mit-Falsch-Kaese-entlarvt-article6750746.html; RTS (2013): Du cheval à la place de boeuf dans des tartares servis en Suisse. https://www.rts.ch/info/suisse/5329304-du-cheval-a-la-place-de-boeuf-dans-des-tartares-servis-en-suisse-.html.
[78] Bundesgesetz über Lebensmittel und Gebrauchsgegenstände vom 9. Oktober 1992 (SR 817.0).
[79] Vgl. Art. 3 und 23 des Bundesgesetzes gegen den unlauteren Wettbewerb vom 19. Dezember 1986 (SR 241); Bundesrat (2011): Botschaft zum Bundesgesetz über Lebensmittel und Gebrauchsgegenstände vom 25. Mai 2011, BBl 2011 5643.
[80] Gewerbsmässig durchgeführte Warenfälschung (Art. 155 Ab. 2 StGB) stellt allerdings ein Verbrechen dar und gilt somit als Vortat zur Geldwäscherei.

bzw. 5% (Kaffee-Kennzeichnungen) der untersuchten Stichproben aus der Schweiz und Liechtenstein ergab sich ein Verdacht auf betrügerische Handlungen.[81] Unregelmässigkeiten werden immer wieder festgestellt, zum Beispiel bei der Vermarktung von Honig[82] oder mit Pestiziden in angeblichen Bio-Getreiden und Müllereierzeugnissen aus verschiedenen osteuropäischen Staaten[83]. Aus Betrügen im Lebensmittelbereich dürfte in der Schweiz jährlich einen Schaden in Millionenhöhe entstehen. In der Europäischen Union werden die wirtschaftlichen Kosten für die Industrie durch betrügerische Praktiken im Lebensmittelbereich auf 8 bis 12 Milliarden Euro geschätzt.[84] Ermittelt wird nur in den wenigsten Fällen. Oft dürfte der Betrug ohnehin unbemerkt bleiben. Es ist aber anzunehmen, dass in der Schweiz inkriminierte Gelder aus Lebensmittelbetrügen gewaschen werden. Eine weitergehende Einschätzung zum Umfang ist aufgrund mangelnder Fakten allerdings nicht möglich.

f) *Weitere betrügerische Phänomene*

Wie bereits erwähnt, ist eine abschliessende Auflistung der Betrugsarten aufgrund der Dynamik dieses Bereichs nicht möglich. Es existieren allerdings noch weitere betrügerische Phänomene zulasten von Unternehmen, die zwar immer wieder vorkommen, aber kein oder nur ein sehr marginales Geldwäschereirisiko für die Schweiz darstellen dürften.

- *Hotelbetrug:* Der Täter weist sich mit falschen Dokumenten aus und verlässt das Hotel, ohne den Aufenthalt zu bezahlen. Eine nachfolgende Geldwäschereihandlung erscheint eher unwahrscheinlich, da das Vorliegen von zu waschenden Vermögenswerten fehlen dürfte.
- *Spielbetrug*: Spielmittel (Karten, Würfeln, usw.) werden gefälscht bzw. gefälschte oder ungültige Lottozettel (oder ähnliches) werden vorgelegt. Solche Taten dürften eher selten vorkommen und vor allem geringfügige Vermögenswerte betreffen.
- *Scheckbetrug*: Der Täter setzt falsche, gefälschte, gestohlene oder ungedeckte Schecks (oder ähnliches) ein. Aufgrund sinkender Beliebtheit von Schecks als Zahlungsmittel dürfte diese Art von Betrug immer seltener vorkommen.[85] Zwischen 2009 und 2018 erhielt MROS insgesamt 39 Geldwäschereiverdachtsmeldungen im Zusammenhang mit Scheckverkehr und Betrug als vermutete Vortat. Scheckbetrüge können im Übrigen auch zulasten Privatpersonen begangen werden.
- Mittels eines sogenannten *Identitätsdiebstahls* bestellen Betrüger Waren unter dem Namen und der Adresse von real existierenden Personen. Sie holen dann die Lieferung an der Adresse des vermeintlichen Bestellers ab. Letzterer bemerkt den Identitätsdiebstahl meistens erst, wenn er eine Rechnung für Waren erhält, die er gar nicht bestellt und erhalten hat. Direkt geschädigt vom Betrug ist rechtlich gesehen grundsätzlich der Lieferant und nicht der angebliche Besteller. Allerdings ist letzterer mit der Schwierigkeit konfrontiert, dem Lieferanten seine Unschuld zu beweisen.

---

[81] Siehe Bundesamt für Lebensmittelsicherheit und Veterinärwesen (2018a): OPSON VII: Wurde der Thunfisch «schöngefärbt»? 04.2018. https://www.blv.admin.ch/dam/blv/de/dokumente/lebensmittel-und-ernaehrung/lebensmittelsicherheit/verantwortlichkeiten/bericht-eu-opson-thunfisch.pdf.download.pdf/Schlussbericht_OPSON_VII_DE.pdf; Bundesamt für Lebensmittelsicherheit und Veterinärwesen (2019): OPSON VIII: Überprüfung von Kaffee-Kennzeichnungen. 06.2019. https://www.newsd.admin.ch/newsd/message/attachments/57406.pdf.

[82] Bundesamt für Lebensmittelsicherheit und Veterinärwesen (2016): Nationale Kampagne zum Nachweis von betrügerischen Praktiken bei der Vermarktung von Honigen und Fischen. https://www.blv.admin.ch/dam/blv/de/dokumente/lebensmittel-und-ernaehrung/lebensmittelsicherheit/verantwortlichkeiten/bericht-nat-kontrollprogramm-betrug-honig-fischen-2015.pdf.download.pdf/Rapport_pour_le_public,_campagne_authenticit%C3%A9_miels_et_poissons,_R%C3%A9sum%C3%A9_D_2.pdf.

[83] Bundesamt für Lebensmittelsicherheit und Veterinärwesen (2018b): Jahresbericht 2017 zu den Kontrollprogrammen an der Grenze. Überwachung von pflanzlichen Lebensmitteln und Gebrauchsgegenständen. https://www.blv.admin.ch/dam/blv/de/dokumente/lebensmittel-und-ernaehrung/lebensmittelsicherheit/verantwortlichkeiten/bericht-grenzkontrollen-2017.pdf.download.pdf/Jahresbericht_Kontrollprogramme_an_der_Grenze_2017_zu_pflanzl._LM_und_GG_DE.pdf.

[84] Europäische Kommission (2018): Knowledge Centre for Food Fraud and Quality. Infographic. https://ec.europa.eu/knowledge4policy/sites/know4pol/files/a0infographic_kc_food_fraud_final_0.pdf.

[85] Siehe Der Bund (2016): Der Check als Auslaufmodell. 23.06.2016. https://www.derbund.ch/wirtschaft/geld/der-check-als-auslaufmodell/story/wirtschaft/geld/der-check-als-auslaufmodell/story/wirtschaft/geld/der-check-als-auslaufmodell/story/17304703.

- *Anstellungsbetrug*: Ein Arbeitgeber stellt infolge einer arglistigen Täuschung einen Arbeitssuchenden an. Auch wenn es theoretisch viele solcher Fälle geben könnte, dürfte diese Art von Betrug in der Praxis selten vor einem Strafgericht landen, da eine zivilrechtliche Lösung (sofortige Kündigung usw.) wohl naheliegender ist. Letzteres dürfte auch bei *Arbeitszeitbetrügen* zutreffen, wo der Arbeitnehmer absichtlich und mit Bereicherungsabsicht höhere Arbeitszeiten angibt als tatsächlich geleistet.

3.2.3 Betrügerische Phänomene zulasten Privatpersonen

Natürliche Personen stellen rein zahlenmässig die grösste potenzielle Opfergruppe dar. Sie können auch bei einigen oben aufgeführten Phänomenen zu den Geschädigten zählen, so insbesondere als private Gläubiger bei Konkursdelikten, bei Scheckbetrügen oder beim Phishing zwecks Missbrauchs einer DVA. Zu den häufigsten betrügerischen Phänomenen zulasten Privatpersonen gehören zudem der Betrug auf Verkaufs- und Immobilienportalen, der Anlagebetrug, der Vorschussbetrug, die falsche Hilfeleistung, der Geldwechselbetrug, die falsche Unterstützungsanfrage, der Heiratsschwindel und der Darlehensbetrug.

a) *Betrug auf Verkaufs- und Immobilienportalen*

Der Handel mit Waren und Dienstleitungen im Internet bietet für Kriminelle verschiedene Betrugsmöglichkeiten; auch Unternehmen lassen sich von falschen Angeboten anlocken. Folgende Maschen zählen zu den in der Schweiz häufig festgestellten Varianten:

- Auf *betrügerischen Internetshops* bieten die Täter Waren bekannter Marken zu sensationell tiefen Preisen an. Die bestellten und bezahlten Einkäufe treffen jedoch nicht bei den Bestellern ein oder die Waren erweisen sich als gefälscht bzw. minderwertig. Die überwiegende Mehrheit dieser Onlineshops werden im Ausland betrieben und der Webauftritt imitiert grösstenteils echte Verkaufsportale. Teilweise nutzen Betrüger auch etablierte Internetauktions-Portale und bieten dort Waren an, die sie in Tat und Wahrheit nicht besitzen. Falls solche Internetseiten in der Schweiz gehostet werden, kann fedpol beim Hosting-Provider mit dem Hinweis auf den betrügerischen Inhalt der Seite einen Antrag auf deren Löschung stellen. Gelöschte betrügerische Verkaufsportale werden jedoch normalerweise rasch unter anderem Namen wieder aufgeschaltet.
- Mit *falschen Immobilienanzeigen* publizieren Betrüger auf Immobilienportalen Anzeigen von oft fiktiven oder nicht zu mietenden Wohnobjekten. Interessenten werden kontaktiert und ihnen wird mitgeteilt, dass sie ausgewählt wurden. Die Täter erfordern allerdings die Vorauszahlung einer Kaution. Ist diese getätigt, verschwinden die Betrüger.
- Durch *fiktive Transportfirmen* bieten die Täter dem Opfer an, eine zuvor auf Kleinanzeigenportalen bestellte Ware zu liefern. Das fiktive Transportunternehmen nimmt anschliessend Kontakt mit dem Opfer auf und verlangt die Vorauszahlung der Transportkosten oder des Verkaufspreises. Ist die Zahlung getätigt, brechen die Betrüger den Kontakt ab und die Ware wird nie geliefert.
- Mit *falschen Zahlungsbestätigungen* sitzen diesmal die Täter auf der Käuferseite. Sie schicken dem Verkäufer ein falsches Mail des gewählten Zahlungsdienstleisters, das bestätigt, dass die Zahlung getätigt oder eingestellt wurde, bis der Versand des Artikels nachgewiesen werden kann. Der Verkäufer versendet die gekaufte Ware, erhält jedoch keine Gegenleistung.

Bei der Studie von Biberstein et al. gaben 2015 8,5% der Befragten an, innerhalb der letzten fünf Jahre Opfer eines Verbraucherschwindels gewesen zu sein.[86] Über ein Viertel der Fälle (28,6%) betrafen dabei Einkäufe im Internet. Hochrechnungen zur Prävalenz solcher Maschen bei der Studie von Beaudet-Labrecque et al. bezifferten 2018 die Anzahl betroffener Personen ab 55 Jahren innerhalb der letzten Jahre auf rund 120’000 bei gefälschten Anzeigen im Internet und auf fast 100’000 beim Betrug bei Online-Zahlungsvorgängen. Dabei hätten fast 50’000

[86] Biberstein et al. (2016), op. cit. S. 16-17.

(bei gefälschten Anzeigen) bzw. über 10'000 (Online-Zahlungen) Personen dieser Altersklasse einen finanziellen Schaden erlitten.[87] 2018 registrierte fedpol zudem 183 Verdachtsmeldungen zur Internetkriminalität wegen falschen Immobilienanzeigen, 267 wegen betrügerischen Internetshops, 260 wegen Produktefälschungen und 63 wegen fiktiven Transportfirmen.

Es ist anzunehmen, dass die jährliche Anzahl durchgeführter Betrüge auf Immobilien- und Verkaufsportalen mindestens im fünfstelligen Bereich liegt; dabei dürften die involvierten durchschnittlichen Summen verhältnismässig tief sein, meistens im drei- bis vierstelligen Bereich. Sofern die Täter gewerbsmässig agieren oder der Schaden 300 Franken übersteigt, dürfte in der Regel eine Geldwäschereihandlung vorliegen.

Fallbeispiel Betrug auf Verkaufsportalen
Der Beschuldigte hatte während kurzer Zeit einer nicht näher identifizierten Person auf deren Wunsch hin sein Konto bei einer Schweizer Bank zur Verfügung gestellt. Er nahm sechs Zahlungen im Gesamtumfang von 2'260 Franken entgegen und leitete die Summen zumindest teilweise via Geldtransferinstitut an seinen Auftraggeber weiter. Dies obwohl er damit rechnen musste, dass die Vermögenswerte deliktischer Herkunft waren. Die Gelder stammten aus verschiedenen Betrugsdelikten auf dem Internet. Der Betrüger und Drahtzieher hatte dabei Smartphones und Handtaschen zum Verkauf angeboten, obwohl er nie die Absicht hatte, die Waren nach Zahlungseingang zu liefern. Der Geldwäscher wurde per Strafbefehl wegen Geldwäscherei zu 240 Stunden gemeinnütziger Arbeit verurteilt. Der Betrüger konnte nicht identifiziert und zur Rechenschaft gezogen werden.

Fallbeispiel Betrug auf Immobilienportalen
Zwei im Ausland wohnhafte Täter, A und B, versuchten im Frühjahr und Sommer 2015 über 200 Wohnungsinserate auf verschiedenen schweizerischen Immobilienportalen zu platzieren. Sie hielten sich dafür mehrere Tage und unter falschen Namen in verschiedenen Hotels in Zürich auf. Die meisten erstellten Inserate wurden von den Portalbetreibern als betrügerisch erkannt und nicht aufgeschaltet. 65 Inserate wurden von diesen Kontrollen nicht entlarvt und wurden publiziert. Darauf meldeten sich über 2000 Interessenten. Die zwei Betrüger, die unter anderem gefälschte Benutzer- und E-Mail-Konten benutzten, nahmen Kontakt mit den Interessenten auf und gaben sich als Besitzer des Wohnobjektes aus. Sie erzählten, dass die Interessenten ausgewählt wurden und verlangten eine Vorauszahlung von einer Monatsmiete und von einem Depot von durchschnittlich über 2'000 Franken. Am Schluss liessen sich elf Interessenten auf das betrügerische Angebot ein. Diese überwiesen das Geld auf ein von einem Finanzagenten kontrolliertes Konto in England. Somit konnten die Täter Vermögenswerte in der Höhe von insgesamt 23'350 Franken entwenden. Einer der Täter erbeutete ausserdem 3'750 Britische Pfund durch den betrügerischen Verkauf eines in Wahrheit fiktiven Jet-Skis auf einem Verkaufsportal. Die zwei Betrüger wurde im März 2017 vom Bezirksgericht Zürich wegen gewerbsmässigen Betrugs, Urkundenfälschung, Geldwäscherei und unlauteren Wettbewerbs zu einer Freiheitsstrafe von 3 Jahren und 6 Monaten bzw. 3 Jahren und 3 Monaten verurteilt.

b) *Anlagebetrug*

Bei einem Anlagebetrug versuchen die Betrüger, ihre potentiellen Opfer mit hohen Gewinnversprechungen zu Investitionen zu bewegen. Dabei werden die Gelder oder andere Vermögenswerte nicht angelegt (oder nur teilweise), sondern sie dienen der Bereicherung der Täter. Es gibt unzählige Varianten dieses Phänomens:

- Viele Betrüge basieren auf einem Umlagesystem (auch *Ponzi-Schema*[88] genannt), wo die Erträge nur oder hauptsächlich durch neue Investoren generiert werden. Lassen sich nicht mehr genügend neue Anleger anwerben, kollabiert das ganze System. Solche Betrüge können sich über Jahre aufrechterhalten, was zu Schadenssummen in Millionenhöhe führen kann. Das Ponzi-Schema wird oft mit sogenannten *Schneeball-*

[87] Beaudet-Labrecque et al. (2018b), op. cit.
[88] Benannt nach Charles Ponzi, welcher die Masche im frühen 20. Jahrhundert in Nordamerika anwendete.

und Pyramidensystemen verwechselt. Bei letzteren sind die Teilnehmer in der Regel bei der Gewinnung neuer Kunden mitinvolviert.[89] Sie wissen, dass deren Erlös vom Anwerben von neuen Anlegern abhängt, was bei einem Ponzi-Schema üblicherweise nicht der Fall ist. Schneeball- und Pyramidensysteme können unter Umständen auch den Betrugstatbestand erfüllen.[90]

- Eine andere Art des Anlagebetrugs stellt der *Boiler-Room*-Betrug dar. Die Täter versuchen meistens per Telefon, potenzielle Opfer von der Investition in (fiktive) Aktien zu überzeugen. Die Kriminellen operieren meist aus Call-Centern im Ausland. Der Begriff *Boiler Room* widerspiegelt dabei sowohl die dortige hektische Stimmung, wie auch den Druck, der auf die Opfer ausgeübt wird. Im Gegensatz zu einem Umlagesystem werden den Opfern eines *Boiler-Room*-Betrugs keine Erträge ausbezahlt oder nur sehr geringe, um diese bei der Stange zu halten.
- Eine weitere Form von Anlagebetrug involviert Kryptowährungen: betrügerische *Initial Coin Offerings* (ICO). Mit einem *Initial Coin Offering* bringen Entwickler ähnlich einem Fundraising das notwendige Kapital auf, um ihre neue Kryptowährung oder Geschäftsidee zu lancieren. Die Anleger stellen dem ICO-Organisator finanzielle Mittel zur Verfügung und erhalten im Gegenzug sogenannte *Token* («Wertmarken») der neuen Währung. Eine betrügerische Form des ICO ist der sogenannte *ICO Exit Scam*. Hierbei gibt die Täterschaft vor, ein neues Unternehmen zu gründen und mit ICO Fundraising zu betreiben. Schliesslich verlässt sie mit den investierten Werten die Umgebung, ohne den Anlegern einen Gegenwert für ihre Einlagen zu hinterlassen.[91]

Bei den meisten Anlagebetrügen geben die Täter vor, in Startups zu investieren, in der medizinischen Forschung oder im Handel mit Aktien, Fonds, Edelmetallen, exotischen Lebensmitteln, erneuerbaren Energien, Rohstoffen, Devisen, Immobilen oder Krypto-Assets tätig zu sein und dabei ein revolutionäres System entwickelt zu haben, das zuverlässig hohe Renditen abwerfe. In Tat und Wahrheit werden die Gelder nicht oder nur teilweise wie versprochen angelegt und stattdessen für den persönlichen, meist sehr aufwändigen Lebensstil der Anlagebetrüger eingesetzt. In vielen Fällen bringen die Täter aus früheren Tätigkeiten Erfahrungen im Finanzwesen mit. In Einzelfällen wurde beobachtet, dass Anlagebetrüger zuvor während Jahren legal als Finanzberater tätig waren und in dieser Funktion relativ erfolgreich Kundengelder angelegt hatten. Dadurch konnten sie sich einen beträchtlichen Stamm an Kunden aufbauen, über deren finanzielle Verhältnisse sie genau im Bild waren. Auf der Suche nach Anlegern für ihr neues, betrügerisches Geschäftsmodell konnten sie innerhalb dieses Kundenstamms mit relativ geringem Aufwand erste zahlungskräftige Investoren gewinnen.

Gemäss der Studie von Beaudet-Labrecque et al. wurden innerhalb der letzten fünf Jahre hochgerechnet über 200'000 der über 55-Jährigen in der Schweiz mit einem betrügerischen Anlagevorschlag konfrontiert; 4 Prozent hätten daraus einen finanziellen Verlust erlitten (ca. 8'600 Personen).[92] Zahlen zur Prävalenz bei den jüngeren Generationen gibt es nicht. Vermutlich werden in der Schweiz jährlich eine vierstellige Anzahl Personen Opfer von Anlagebetrügern; dabei können die finanziellen Schäden von Fall zu Fall sehr unterschiedlich ausfallen. Bei der Variante *Boiler Room* wurden gemäss Daten von fedpol zwischen 2010 und 2017 in der Schweiz mindestens 91 Millionen Franken erbeutet; die tatsächlich entwendete Summe dürfte allerdings aufgrund einer vermutlich hohen Dunkelziffer um einiges höher liegen. Die Schadensumme pro Opfer variierte stark, von einigen tausenden Franken bis zu mehreren

[89] Siehe Bundesrat (2009): Botschaft zur Änderung des Bundesgesetzes gegen den unlauteren Wettbewerb (UWG) vom 2. September 2009, BBl 2009 6176.
[90] Balzli, Tina (2018): *Art. 3 Abs. 1 lit. r*, in: Heizmann, Reto / Loacker, Leander D. (Hrsg.): UWG Bundesgesetz gegen den unlauteren Wettbewerb. Kommentar. Zürich 2018, S. 718-719.
[91] Vgl. auch KGGT (2018b): Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding. Oktober 2018.
[92] Beaudet-Labrecque et al. (2018b), op. cit.

Millionen. Bei den betrügerischen ICO ist insbesondere Ethereum[93] anfällig, da 82 % aller ICO auf der Ethereum Blockchain erfolgen. Auch hat der Trend zu den ICO in Form dezentralisierter Investitionen in den Jahren 2017 und 2018 zugenommen.[94] Es ist anzunehmen, dass aus den meisten vollzogenen Anlagebetrügen, auch aus solchen, die Krypto-Assets involvieren, Geldwäschereihandlungen entstehen.

Fallbeispiel Anlagebetrug
Der Texaner Allen Stanford betrieb in den USA während mehr als 20 Jahren ein Anlagebetrugsschema das punkto Ausmass bislang nur von jenem von Bernard Madoffs übertroffen wurde. Durch den Verkauf von sogenannten Einlagezertifikaten (certificates of deposit), die gemäss Stanfords Versprechungen garantierte jährliche Renditen im zweistelligen Prozentbereich abwerfen sollten, nahm er Anlagekapital im Umfang von rund acht Milliarden Dollar entgegen und finanzierte anfallende Renditeauszahlungen mit neuen Kundengeldern. Mit Hilfe eines kleinen Führungszirkels, bestehend aus Familienangehörigen und engen Freunden, baute Stanford ein komplexes, internationales Firmengeflecht auf, dem auch die in der Schweiz ansässige Stanford Group (Suisse) AG angehörte. Allen Stanford wurde 2012 in den USA zu einer Gefängnisstrafe von 110 Jahren verurteilt.
Die bis zu ihrer Liquidation in Zürich domizilierte Stanford Group (Suisse) AG wurde 1997 gegründet und war gemäss Handelsregistereintrag hauptsächlich in der Vermögensberatung und -verwaltung tätig. Nachdem 2009 in den USA ein Verfahren gegen Allen Stanford und seine Mitarbeiter eingeleitet wurde, gingen bei MROS mehrere Meldungen von Schweizer Finanzintermediären ein, die Kontobeziehungen zur Stanford Group (Suisse) AG unterhielten. Die Bundesanwaltschaft eröffnete daraufhin ein Verfahren wegen Geldwäscherei und blockierte Vermögenswerte im Umfang von über 200 Millionen Schweizer Franken. Wenige Monate nach der Eröffnung des Verfahrens in den USA beschloss der Verwaltungsrat der Stanford Group (Suisse) AG die ordentliche Auflösung der Gesellschaft. 2014 konnte die Bundesanwaltschaft ihre Untersuchungen in dieser Sache abschliessen. Mit Unterstützung der amerikanischen Justizbehörden gelang es ihr darzulegen, dass ein Teil der in die Schweiz geflossenen Gelder aus dem Anlagebetrug in den USA stammte. Da sich die Hauptbeschuldigten bereits in den USA für ihre Taten verantworten mussten, wurden die Verfahren gegen sie in der Schweiz eingestellt. Hingegen verurteilte die Bundesanwaltschaft die Stanford Group (Suisse) AG wegen qualifizierter Geldwäscherei mittels Strafbefehl und unter Anwendung der Unternehmungshaftung gemäss Art. 102 Abs. 2 StGB zu einer Busse von einer Million Schweizer Franken und bestimmte als Ausgleich für die deliktisch erlangten Gewinne eine Ersatzforderung im oberen einstelligen Millionenbereich. Die Busse und die Ersatzforderung kamen den Geschädigten des Anlagebetrugs zugute.[95]

c) *Falsche Unterstützungsanfrage*

Bei falschen Unterstützungsanfragen geben sich die Täter als Bekannte der Opfer aus und behaupten sie seien in Geldnot. Es gibt dabei unzählige Varianten, die je nach Tatablauf auch als Vorschussbetrug qualifiziert werden können.

- Eine der bekanntesten Varianten ist der *Enkeltrick*. Die Täter geben sich als Verwandte oder nahe Bekannte des Opfers aus und geben vor, sich in finanzieller Notlage zu befinden. Ist das Opfer bereit, finanzielle Hilfe zu leisten, gibt der vermeintliche Verwandte oder Bekannte vor, das Geld aus terminlichen Gründen nicht persönlich abholen zu können. Stattdessen schickt er eine angebliche Vertrauensperson, die das Geld in bar abholt. Der Enkeltrick ist eine Spielart des Telefon- oder Callcenter-Betrugs zulasten Privatpersonen.

[93] Ethereum ist eine in Zug ansässige Stiftung, die seit 2015 u.a. das auf die sogenannte Blockchain-Technologie basierte Ethereum Protokoll fördert. Die Kryptowährung vom Ethereum heisst Ether (ETH).
[94] Chainalysis (2019): Crypto Crime Report. Decoding Hacks, Darknet Markets, and Scams, S. 16. https://blog.chainalysis.com/.
[95] Bundesanwaltschaft (2014): Schweiz entschädigt Opfer im Fall Allen Stanford. https://www.news.admin.ch/message/index.html?lang=de&msg-id=52261.

- Bei der Cybervariante gelangen die Täter meistens durch Hacking in die E-Mailkonten von Dritten und senden in deren Namen an deren Kontakte falsche Unterstützungsanfragen. Sie behaupten beispielsweise, Opfer eines Angriffs im Ausland geworden zu sein und das ganze Geld sowie die Identitätspapiere verloren zu haben. Sie bitten um finanzielle Hilfe und versprechen, die Beträge nach ihrer Rückkehr zurückzuzahlen. Üblicherweise werden die Opfer gebeten, das Geld via Geldtransferinstitut zu versenden, da dies am schnellsten gehe.
- Falsche Unterstützungsanfragen können auch klassisch erfolgen, das heisst ohne Hilfe vom Internet. Die Täter erzählen den Opfern von einer angeblichen Notsituation, beispielsweise von schwerkranken Kindern und bitten um Geld.

Polizeiliche Ermittlung haben gezeigt, dass Enkeltrickbetrüger sehr gut organisiert sind und arbeitsteilig vorgehen. Es wird geschätzt, dass europaweit eine tiefe vierstellige Anzahl Täter aktiv ist. Die meisten Enkeltrickbetrüger stammen aus Süd- und Zentraleuropa.

Der Studie von Beaudet-Labrecque et al. zufolge dürfte es in der Schweiz jährlich über 20'000 Enkeltrickversuche geben, davon über 400 mit finanziellem Verlust.[96] Bei fedpol werden seit 2011 jährlich durchschnittlich 600 Enkeltrickversuche gemeldet, davon waren rund 10% aus Sicht der Täter erfolgreich. Die durchschnittliche Schadensumme pro gemeldeten Fall lag bei 45'000 Franken. Beim erfolgten Enkeltrick dürfte oft eine Geldwäschereihandlung vorliegen, da die Täter das Geld üblicherweise bar über die Grenze transportieren. Schätzungen betreffend die Anzahl falscher Unterstützungsanfragen über das Internet in der Schweiz existieren nicht. Jährlich erhält fedpol zu dieser Variante des Phänomens Verdachtsmeldungen zur Internetkriminalität im zwei- bis tiefen dreistelligen Bereich (2018: 21 Verdachtsmeldungen); die entwendeten Summen sind deutlich tiefer als beim Enkeltrick und liegen üblicherweise im dreistelligen Bereich.

d) *Falsche Hilfeleistung*

Im Gegensatz zur falschen Unterstützungsanfrage täuschen die Täter im Falle von falscher Hilfeleistung eine Not- oder Problemsituation bei den Opfern selbst vor. Zu häufigen Varianten zählen der Betrug mit dem falschen Polizeibeamten und die falschen Support-Anrufe.

- Beim *Betrug mit dem falschen Polizeibeamten* geben sich die Täter als Polizisten aus und behaupten, Gelder oder Wertgegenstände der Geschädigten seien aus verschiedenen Gründen nicht mehr sicher. Es komme deshalb ein Polizeibeamter vorbei, um es in Sicherheit zu bringen.
- Bei *betrügerischen Support-Anrufen* geben sich die Täter als Techniker der Firma Microsoft, Apple und dergleichen aus. Sie versuchen mit verschiedenen Tricks, einen Fernzugriff auf den Computer des Opfers zu erhalten, um daraus einen finanziellen Vorteil zu erlangen. Je nach Situation verlangen sie auch eine Beratungsgebühr für die Beseitigung eines angeblichen Computerproblems oder bieten den Abschluss eines Support-Abonnements beziehungsweise den Kauf von Software-Lizenzen an.

Opferbefragungen zufolge dürfte es in der Schweiz jährlich über 4'000 Versuche mit falschen Polizeibeamten geben.[97] Dieses Phänomen hat in den letzten Jahren zugenommen. Die bei fedpol gemeldeten Fälle (inkl. Versuche) nahmen von 29 im Jahr 2016 auf 2'560 im Jahr 2018 zu; dabei lag die Erfolgsquote unter 2%. Die durchschnittliche Schadensumme pro Fall war verhältnismässig hoch und betrug 105'000 Franken. Online registriert fedpol zudem jährlich zwischen 200 und 500 Verdachtsmeldungen zur Internetkriminalität, die als Support-Anrufe klassifiziert werden können; die Deliktsumme bei letzterer Variante bleibt allerdings meistens im dreistelligen Bereich.

[96] Beaudet-Labrecque et al. (2018b), op. cit.
[97] Beaudet-Labrecque et al. (2018b), op. cit.

e) *Vorschussbetrug*

Bei diesem Modus Operandi versenden die Täter E-Mails, SMS, Instant Messages – früher auch Briefe – in denen sie potenziellen Opfern hohe Gewinne bzw. Kommissionen versprechen. Um die Summen auszulösen, müssten aber Vorschusszahlungen geleistet werden. Den Gewinnversprechungen liegen immer wieder neue Legenden zugrunde. Verbreitete Versionen sind:

- *Das grosse Erbe*: Die Täter geben an, das Opfer habe eine hohe Summe geerbt. Für deren Freigabe müssten aber noch Notariatsgebühren, Transferkosten, Steuern, etc. bezahlt werden. Für die Deckung dieser Kosten versprechen sie einen Anteil am Erbe.
- *Das nachrichtenlose Vermögen*: Die Täter geben sich als Angestellte einer afrikanischen Bank aus, die ein nachrichtenloses Vermögen aufgespürt haben. Um sich die Gelder anzueignen, brauchen sie angeblich einen Partner im Ausland, der sein Bankkonto zur Verfügung stellt und zudem in der Lage ist, verschiedene administrative Kosten zu decken.
- *Der Lottogewinn*: Die potenziellen Opfer werden darüber informiert, dass sie im Lotto gewonnen haben. Bevor der Lottogewinn ausbezahlt werden kann, fallen aber Gebühren an.

Hat ein Opfer angebissen, wird es von den Tätern angewiesen, persönliche Dokumente einzureichen und – gewöhnlich via Geldtransferinstitute – Zahlungen zu tätigen. Wenn die ersten Kosten bezahlt sind, werden neue Vorwände erfunden, um weitere Gelder einzufordern. Immer wieder bezahlen Schweizer Opfer tausende Franken ohne die versprochenen Gewinne jemals zu erhalten.

Punktuelle Ermittlungen von Schweizer Strafverfolgungsbehörden haben gezeigt, dass Tätergruppierungen dabei wie eine Art Untergrund-Marktwirtschaft funktionieren, in der Dienstleistungen und Produkte in der Regel über einschlägige Internetforen gehandelt werden *(Crime-as-a-Service)*. Eine erste Täterschaft bietet beispielsweise ein Netz infizierter Computer an, über die die Spam-Mails verschickt werden können. Eine zweite Täterschaft schreibt die Texte und stellt den Kontakt zu den potenziellen Opfern her. Wieder andere Täter spezialisieren sich auf die Herstellung gefälschter Dokumente und Urkunden, die an die Opfer weitergeleitet werden können, um damit die Existenz des Lottogewinns oder der Erbschaft scheinbar zu belegen. Sobald die ersten Gelder fliessen, braucht es zudem Personen, die die Summen bei den Geldtransferinstituten abholen und an die Hintermänner weiterleiten. Auch die Dienste dieser Finanzagenten werden auf den Internetforen angeboten. Schliesslich werden Personen, die in der Vergangenheit bereits auf Betrugsmails geantwortet haben, auf Listen vermerkt. Diese Listen werden weiterverkauft, in der Hoffnung, dass die Personen auch ein zweites Mal auf einen Betrugsversuch hereinfallen. Die verschiedenen Anbieter dieser Produkte und Dienstleistungen kennen sich oft nicht oder nur flüchtig über Internetforen und sind nur lose miteinander verbunden. Die Netzwerke funktionieren sehr flexibel. Je nach Verfügbarkeit werden die Anbieter ausgewählt und deren Dienste eingekauft.

Versuche von Vorschussbetrug sind in der Schweiz sehr häufig. Allerdings schlagen sie meistens fehl. Bei der Studie von Beaudet-Labrecque et al. lag 2018 die Erfolgsquote bei knapp über 2%. Hochgerechnet entsprach dies rund 8'600 Personen ab 55 Jahren, welche aufgrund dieser Masche innerhalb der fünf letzten Jahre einen finanziellen Schaden erlitten haben.[98] Ähnliche Daten zu den anderen Altersklassen existieren nicht.

Es ist anzunehmen, dass die tatsächliche Anzahl erfolgreicher Vorschussbetrüge jährlich im vierstelligen Bereich liegt und meistens drei- bis vierstellige Summen involviert sind. Da die Täter oft im Ausland sitzen, müssen die Gelder in der Regel über Finanzintermediäre transferiert werden; nicht selten werden auch Finanzagenten eingesetzt, um den *Paper Trail* zu unterbrechen. Eine Geldwäschereihandlung dürfte somit bei vielen vollzogenen Vorschussbetrügen vorliegen (Gegenbeispiel: cf. Kasten).

[98] Beaudet-Labrecque et al. (2018b), op. cit.

Fallbeispiel Vorschussbetrug
Ein Geldüberweisungsinstitut erstattete eine Geldwäschereimeldung, weil ein Kunde im Zeitraum von rund einem Jahr insgesamt 53 Überweisungen im Gesamtwert von 14'324 Franken an 13 Empfänger in fünf Ländern getätigt hatte. Aufgefallen waren die Transaktionen als der Beschuldigte eine Überweisung an einen Empfänger veranlasste, der in der Vergangenheit bereits von einem anderen Kunden Geld erhalten hatte. Der Beschuldigte wurde gebeten, den Grund für die Überweisungen anzugeben und Unterlagen zur Herkunft der Gelder (Lohnabrechnung, Kontoauszug etc.) einzureichen, was dieser jedoch verweigerte. Aufgrund der Verdachtsmeldung eröffnete die zuständige kantonale Staatsanwaltschaft ein Verfahren wegen Geldwäscherei gegen den Beschuldigten. Bei der Einvernahme sagte letzterer schliesslich aus, dass die nach Spanien und in verschiedene afrikanische Länder transferierten Gelder aus seinen eigenen Mitteln stammen. Er habe im Internet nach Verdienstmöglichkeiten gesucht und sei daraufhin von Personen aus dem Ausland kontaktiert worden. Diese hätten ihm Geschäfte vorgeschlagen, bei denen er jedoch Vorschusszahlungen leisten musste. Für die Ermittler lag rasch auf der Hand, dass der Beschuldigte Opfer eines Vorschussbetrugs geworden war. Da die Gelder nachweislich aus legaler Herkunft stammten, wurde das Verfahren wegen Geldwäscherei gegen den Beschuldigten eingestellt.

f) *Geldwechselbetrug*

Bei einem Geldwechselbetrug versuchen die Täter die Opfer in ein Geschäft zu verwickeln und im Zuge der Abwicklung falsches gegen echtes Geld zu tauschen. Es gibt verschiedene Varianten:

- Beim *Rip-Deal* versuchen die Kriminellen, Personen mit hohen Gewinnver-sprechungen anzulocken und zu einem – betrügerischen – Devisentausch zu überreden. Bei der Geldübergabe oder auch bei einer Bitcointransaktion wird das Opfer dann aber um sein Geld betrogen, indem es meistens Falschgeld erhält. Je nach Tatkonstellation entfällt der Betrug zugunsten des Diebstahls. Unternehmen können auch zu den Geschädigten zählen.
- Beim *Wash-Wash-Betrug* gaukeln die Täter den Opfern vor, sie könnten mit einer chemischen Flüssigkeit Geld vermehren oder verfärbte (angebliche) Banknoten wieder waschen. Dem Opfer wird ein Teil des Ertrags versprochen, dafür hat es indes einen Vorschuss zu leisten. Es existieren zahlreiche Varianten der Betrugsmasche, welche unter Umständen auch als Vorschussbetrug qualifiziert werden können.
- Beim einfachen *Währungstausch* wird das Opfer auf der Strasse spontan angefragt, ob er eine Fremdwährung tauschen könne. Im Gegenzug erhält der Passant meist Falschgeld oder die Täter nutzen die Gelegenheit aus, um Geld aus dem Portemonnaie zu stehlen, was in dem Fall als Trickdiebstahl gelten würde.

Vor allem Geldwechselbetrüge in der Variante *Rip-Deal* und *Wash-Wash* sind in der Regel der organisierten Kriminalität zuzurechnen. Beim *Rip-Deal* sind die meisten Taten auf die gleichen kriminellen Grossfamilien zurückzuführen, welche ursprünglich aus Südosteuropa stammen und mittlerweile in den meisten Staaten Süd- und Mitteleuropas ansässig sind. Der *Wash-Wash*-Betrug wird oft von Gruppierungen aus Westafrika begangen. In beiden Fällen gehen die Täter international und arbeitsteilig vor.

Die Studie von Beaudet-Labrecque et al. rechnet hoch, dass innerhalb der letzten fünf Jahre rund 170'000 Personen ab 55 Jahren mit einem betrügerischen Währungstausch konfrontiert waren; 23'000 von ihnen hätten im gleichen Zeitraum einen finanziellen Nachteil erlitten.[99] Diesem dürfte aber teilweise ein Diebstahl und nicht ein Betrug zugrunde liegen. Jährlich werden fedpol zwischen 20 und 50 *Rip-Deal*-Fälle gemeldet, wovon jeweils 10 bis 20 vollendet wurden. Die durchschnittliche Schadensumme pro gemeldeten Fall liegt über 400'000 Franken und ist

[99] Beaudet-Labrecque et al. (2018b), op. cit.

damit verhältnismässig hoch. Gesamtzahlen zum *Wash-Wash* existieren nicht; diese Betrugsart dürfte allerdings auch eher ein Nischendelikt sein. Da die Täter oft die inkriminierten Vermögenswerte bar über die Grenze transportieren, liegt, sofern der Betrugstatbestand erfüllt ist, meistens auch eine Geldwäschereihandlung vor. Sollte das Geld, das vom Opfer zum Austausch angeboten wird, aus einem Verbrechen oder einem qualifizierten Steuervergehen stammen, würde der *Rip-Deal* selbst als (misslungene) Geldwäschereihandlung fungieren. Solche Fälle bringen die – vermutlich nicht allzu seltenen – Opfer in der Regel nicht zur Anzeige.

g) *Heiratsschwindel (Romance Scam)*

Beim Heiratsbetrug täuscht der Täter eine Liebesbeziehung vor, um daraus einen finanziellen Vorteil zu erlangen. Die über das Internet durchgeführte Variante wird oft als *Romance Scam* bezeichnet. Die Kontaktanbahnung findet über Online-Dating-Plattformen, über soziale Netzwerke, Chatrooms, etc. statt. Nach einem langwierigen Austausch per E-Mail, Briefe oder am Telefon versuchen die Kriminellen, das Opfer zu animieren, Geld zu überweisen. Typische Ausrede ist zum Beispiel einen Besuch beim Opfer, welcher aber in der letzten Minute doch noch «scheitert» oder angebliche medizinische Komplikationen in der Verwandtschaft, die dringend Geld erfordern. Die Geldüberweisungen finden oft über Zahlungsdienstleister statt. Sobald der Betrüger sein Ziel erreicht hat bzw. ab dem Moment wo sein Opfer die Zahlungen einstellt, verschwindet er. Hinter dieser Masche stecken oft organisierte Gruppierungen aus Westafrika; andere Herkunftsregionen werden aber ebenfalls beobachtet.

In der Studie von Beaudet-Labrecque et al. wurde 2018 die Anzahl Opfer ab 55 Jahren, die innerhalb der fünf letzten Jahre mit einem *Romance Scam*-Versuch konfrontiert waren, auf fast 40’000 Personen geschätzt; gemäss gleicher Studie haben mutmasslich 15’000 unter ihnen einen finanziellen Verlust erlitten.[100] Die Schadensumme kann dabei erheblich variieren; in manchen Fällen handelt es sich um hohe fünfstellige Beträge. Vergleichbare Daten für die anderen Altersgruppen existieren nicht. Da die Gelder meistens ins Ausland transferiert werden, dürfte bei einem erfolgreichen Heiratsbetrug oft eine Geldwäschereihandlung vorliegen.

h) *Darlehensbetrug*

Im Gegensatz zum Kreditbetrug sitzt beim Darlehensbetrug der Betrüger auf der Seite der Geldverleiher. Er verspricht dem Opfer ein Darlehen, verlangt aber für die Vermittlung eine Provision, die das Opfer im Voraus entrichten soll. Sobald diese Zahlung getätigt wird, bricht der Täter den Kontakt ab, ohne das Darlehen zu gewähren.

Zuverlässige Zahlen zum Ausmass dieses Phänomens liegen fedpol nicht vor. Vermutlich liegt die jährliche Anzahl Fälle im dreistelligen Bereich.

i) *Betrug beim Warenerheben oder Warenverkauf*

Beim Betrug beim Warenerheben oder Warenverkauf werden entweder minderwertige, falsche oder gefälschte Waren verkauft oder letztere werden betrügerisch von den Tätern ohne jegliche Zahlungsabsicht in Besitz genommen (zum Lebensmittelbetrug und zur Variante über Verkaufsportalen siehe die entsprechenden Unterkapitel oben). Solche Fälle kommen relativ häufig vor; viele dürften allerdings als geringfügige Vermögensdelikte gelten und somit keine Vortat zur Geldwäscherei bilden. Solche Betrüge können auch zulasten eines Unternehmens begangen werden.

Eine Sondervariante stellt der *Betrug beim Fahrzeugerheben oder -verkauf* dar. Dabei werden gemietete, entwendete, manipulierte oder fehlerhafte Fahrzeuge verkauft bzw. Fahrzeuge werden ohne Zahlungsabsicht erhoben. Die 2015 öffentlich bekannt gewordene Abgasmanipulationen beim deutschen Konzern Volkswagen AG hat gezeigt, dass potenzielle Betrüge in diesem Bereich schnell ein grosses Ausmass annehmen können. Die Bundesanwaltschaft führt seit 2016 ein Strafverfahren gegen die Volkswagen AG in Deutschland, die involvierte Importfirma in der Schweiz sowie deren verantwortlichen Organe und Betriebszugehörigen

[100] Beaudet-Labrecque et al. (2018b), op. cit.

wegen Verdachts des gewerbsmässigen Betrugs. Ihnen wird vorgeworfen, teilweise im Wissen um die vorgenommenen Abgasmanipulationen, rund 175'000 Käufer und Leasingnehmer von Fahrzeugen geschädigt zu haben.[101] Inwiefern dabei Geldwäschereihandlungen stattfanden, lässt sich zurzeit nicht sagen.

j) *Weitere betrügerische Phänomenen*

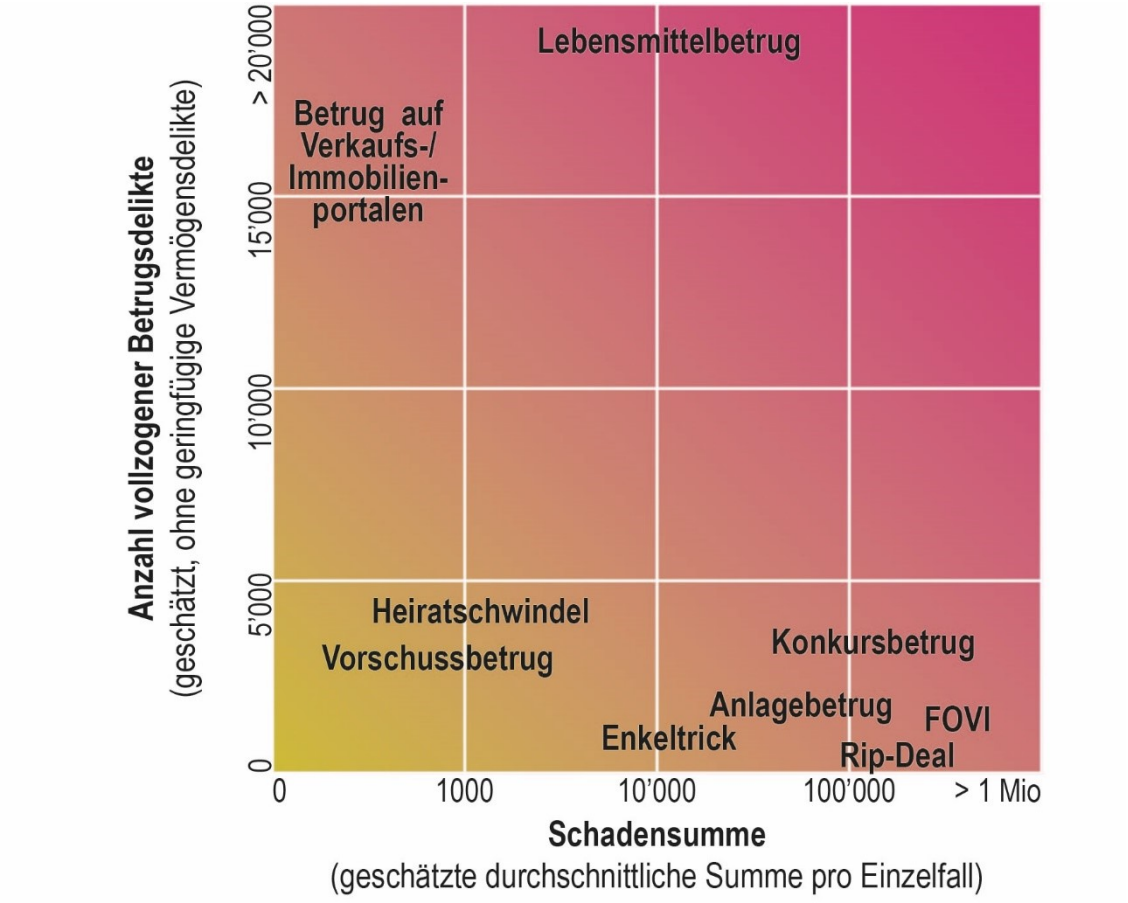
Die Anzahl Betrugsphänomene zulasten von Privatpersonen kann nicht abschliessend aufgeführt werden. Erwähnenswert, weil häufig, sind der *Bettel- und Spendenbetrug*. Es gibt verschiedene Variante dieser Betrugsart. Häufig geben sich die Täter als Menschen mit Behinderungen aus und sammeln Geld für meist fiktive karitative Hilfswerke. Ebenfalls verbreitet ist der sogenannte Benzintrick. Dabei stehen die Täter neben ihrem Fahrzeug am Strassenrand und halten Automobilisten an, um sie nach Geld für Benzin anzugehen, das schliesslich nicht rückerstattet wird. Solche Taten werden meistens als Bagatelldelikt behandelt. Allerdings liegen konkrete polizeiliche Hinweise vor, dass ein Teil der Bettel- und Spendenbetrüge in der Schweiz durchaus organisiert sind. Die daraus zu waschenden Vermögenswerte dürften aber vergleichsweise bescheiden sein.

3.2.4 Bewertung der Gefährdung durch besondere Betrugsphänomene

Die analysierten Betrugsphänomene weisen grosse Unterschiede auf. Sie zielen auf verschiedene Opfer und Opfergruppen, verlangen mehr oder weniger komplexe Tathandlungen und erzielen disparate Erfolge. Bemerkenswert bei den verschiedenen Vorgehensweisen ist das Verhältnis zwischen der Anzahl potentieller Opfer und den Erträgen, die erzielt werden können: Einerseits finden Betrüge statt, die massenhaft und mit relativ wenig Aufwand durchgeführt werden können, die im Durchschnitt aber auch weniger kriminelle Erträge pro Fall einbringen. Typische Beispiele dafür sind Betrüge auf Onlineshops oder Immobilienplattformen, wo die Schadensumme pro Opfer meistens im zwei- oder dreistelligem Bereich liegt. Anderseits gibt es Modi Operandi, die zahlenmässig seltener gelingen dürften, die aber den Kriminellen hohe Erträge versprechen. Dafür müssen die Täter im Schnitt mehr Zeit investieren, wie beispielsweise bei falschen Hilfeleistungen oder falschen Überweisungsaufträgen. In solchen Betrugsfällen beträgt die fallbezogene Schadensumme regelmässig mehrere hunderttausend

[101] Bundesanwaltschaft (2019): VW-Abgasmanipulationen: Online-Fragebogen für Geschädigte. Medienmitteilung vom 02.09.2019. https://www.bundesanwaltschaft.ch/mpc/de/home/medien/archiv-medienmitteilungen/news-seite.msg-id-76267.html.

Franken. Eine Ausnahme bilden die Betrüge im Lebensmittelbereich, die mit geringem Aufwand durchgeführt werden und je nach Konstellation hohe kriminelle Erträge generieren können.



Grafik 8: Betrügerische Delikte nach ihren geschätzten Vorkommen und Schadensummen. Bei einigen Phänomenen liegen keine Schätzungen vor.

Die potenzielle Gefährdung ist somit bei Betrugsarten am höchsten, die entweder eine grosse Anzahl Personen betreffen oder pro Einzelfall hohen Schaden verursachen. Eine Kombination dieser beiden Kriterien ist bis anhin nur beim Lebensmittelbetrug zu vermuten, allerdings sind die Daten in diesem Bereich noch sehr dürftig. Pro Einzelfall ist die potenzielle Geldwäschereigefährdung bei den falschen internationalen Überweisungsaufträgen, bei gewissen Geldwechselbetrügen (insb. beim *Rip-Deal*) und bei vielen Anlagebetrügen am höchsten. Dort werden verhältnismässig hohe Beträge entwendet und anschliessend gewaschen. Betrüge auf Verkaufs- und Immobilienportalen stellen vor allem in ihrer Gesamtheit eine erhöhte Gefährdung dar. Aus dem Phishing selbst entsteht keine Geldwäschereigefährdung, da in der Regel noch kein Vermögen tangiert ist. Erst die anschliessend, meist durch den betrügerischen Missbrauch einer DVA, erlangten Vermögenswerte bilden eine Vortat zur Geldwäscherei. Das Ausmass dieser Gefährdung ist aber aufgrund mangelnder Daten schwer einzuschätzen. Rechnet man die Schätzung der Zürcher Strafbehörden zum Konkursbetrug auf die ganze Schweiz hoch, stellt dieses Betrugsphänomen mit einer jährlichen Schadensumme von über einer Milliarde Franken ebenfalls eine finanziell gesehen potenzielle hohe Gefährdung dar. Insgesamt sind die Schadensummen beim Staat und bei Unternehmern durchschnittlich um einiges höher als bei privaten Personen.

4 Verwundbarkeiten und Herausforderungen

Die allgemeinen Verwundbarkeiten sind bei Geldwäschereihandlungen mit Vortat Betrug und Missbrauch einer DVA grundsätzlich die gleichen wie bei anderen Vortaten. Als Land mit wichtigem Finanzsektor ist die Schweiz dem potenziellen Missbrauch ihres Finanzplatzes zu Geldwäschereizwecken ausgesetzt. Dies betrifft auch Geldwäschereihandlungen mit Vortat Betrug. Die schon veröffentlichten NRA-Berichte haben aber gezeigt, dass sich die allgemeinen Verwundbarkeiten des Landes in Bezug auf Geldwäscherei dank einem umfassenden, koordinierten und wirksamen rechtlichen und institutionellen Geldwäschereibekämpfungssystem in Grenzen halten. Auf die allgemeine Verwundbarkeit wird aus diesem Grund hier nicht weiter eingegangen; es wird auf die schon publizierten NRA-Berichte verwiesen.[102]

Dieses Kapitel ist vor allem den spezifischen Verwundbarkeiten sowie den Verwundbarkeiten in Verbindung mit dem institutionellen Dispositiv gewidmet, da diese bei den Betrugsdelikten gewisse Besonderheiten aufweisen. Solche Verwundbarkeiten sind gleichwohl eine Herausforderung für die Strafbehörden.

4.1 Spezifische Verwundbarkeiten

Die spezifischen Verwundbarkeiten sind mit den Praktiken und Instrumenten verbunden, die in einem bestimmten Tätigkeitsbereich verwendet werden. Bei Betrugsdelikten liegen solche Verwundbarkeiten vor allem bei der Verwendung von Bargeld und von informellen Überweisungssystemen, dem Einsatz von Finanzagenten und juristischen Personen mit Sitz im Ausland sowie den dank der neueren Informations- und Kommunikationstechnologien vermehrten Möglichkeiten zur Internationalisierung der Straftaten und der damit verbundenen Geldwäscherei. Informationen über den Einsatz von Krypto-Assets zum Zwecke der Geldwäscherei nach Betrugsdelikten sind noch lückenhaft; solche Technologien stellen aber potenziell eine grosse Verwundbarkeit dar.

4.1.1 Bargeld

Das Risiko, dass Bargeld für Geldwäschereizwecke in der Schweiz missbraucht wird, ist gemäss dem NRA-Bericht über die Bargeldverwendung moderat.[103] Allerdings wurde beim Betrug und insbesondere bei gewissen Onlinebetrügen wiederholt der Einsatz von Bargeld festgestellt. Auch die im vorliegenden Bericht analysierten Fälle zeigen, dass bei gewissen Phänomenen häufig Bargeld verwendet wird. Dies betrifft zum einen die Betrugsvarianten Enkeltrick und falsche Polizeibeamte sowie den Geldwechselbetrug, in welchen hauptsächlich bares Geld physisch über die Grenze gebracht wird. Bei digitalen Betrügen versuchen die Täter mit dem Einsatz von Finanzagenten den *Paper Trail* zu unterbrechen, indem letztere das überwiesene Geld abheben und entweder auf neue Konten einzahlen oder sogar per Postdienst in Couverts oder Pakete bar weiter versenden.

4.1.2 Informelle Überweisungssysteme

Informelle Überweisungssysteme kommen ursprünglich oft aus Regionen, in welchen der Bankensektor nicht stark etabliert ist oder nicht funktioniert. Sie werden auch verwendet, um kriminelle Geschäfte abzuwickeln. Solche Systeme, wie etwa das sogenannte Hawala, basieren auf Ausgleichmechanismen und sind meistens auf ethnisch, ideologisch oder religiös homogene Gruppen beschränkt. Die Spuren der Gelder sind umso schwerer zurückzuverfolgen, da physisch meistens keine Transaktion stattfindet, sondern zwischen den verschiedenen

[102] Vgl. unter anderem KGGT (2018a): Bericht über die Bargeldverwendung und deren Missbrauchsrisiken für die Geldwäscherei und Terrorismusfinanzierung in der Schweiz. Oktober 2018. https://www.newsd.admin.ch/newsd/message/attachments/55177.pdf; KGGT (2018b), op. cit. https://www.newsd.admin.ch/newsd/message/attachments/56167.pdf; KGGT (2017): Geldwäschereirisiken bei juristischen Personen. November 2017. https://www.fedpol.admin.ch/dam/data/fedpol/kriminalitaet/geldwaescherei/nra-berichte/nra-bericht-nov-2017-f.pdf; KGGT (2015a), op. cit.

[103] KGGT (2018a), op. cit.

«Dienstleistern» kompensiert wird. Der Einsatz solcher informellen Systeme wird vor allem beim Phänomen falsche internationale Überweisungsaufträge vermutet, konnte aber bislang nicht bewiesen werden.

4.1.3 Juristische Personen mit Sitz im Ausland

Ausländische kaufmännische Rechtsträger stellen grundsätzlich ein grösseres Geldwäschereirisiko dar als schweizerische, dies unabhängig von ihrer Rechtsform.[104] Auch Trusts können als Instrument für Geldwäschereizwecke missbraucht werden. Betrug spielt zwar als häufigste bzw. zweithäufigste vermutete Vortat sowohl bei den schweizerischen als auch bei den ausländischen Rechtsträgern eine wichtige Rolle. Dank eines grundsätzlich wirksamen Abwehr- und Bekämpfungsdispositivs, insbesondere der Sorgfaltspflichten der Finanzintermediäre, kann das Risiko für hiesige Gesellschaften aber deutlich reduziert werden.

Bei den ausländischen kaufmännischen Rechtsträger besteht die Verbindung zur Schweiz in der Regel aus hier eröffneten Bankkonten. Gemäss der Verdachtsmeldungsstatistik von MROS (cf. Kapitel 3.1.4) sind 20% der Vertragsparteien mit vermuteter Vortat Betrug (2016-2018) ausländische juristische Personen. Über zwei Drittel (72%) davon waren Sitzgesellschaften, vor allem mit Sitz in Zentralamerika und der Karibik (63% aller ausländischen Sitzgesellschaften) sowie in Osteuropa (24%). Der Wohnsitz des wirtschaftlich Berechtigten (WB) von Sitzgesellschaften liegt regelmässig in einer anderen Weltregion als der Sitz seiner Gesellschaft, meistens in Osteuropa (27% aller WB mit einer Sitzgesellschaft als Vertragspartei) und in den postsowjetischen Staaten (23%) sowie im Nahen und Mittleren Osten (13%). Dies erhärtet den Verdacht, dass Sitzgesellschaften verwendet werden, um betrügerisch erlangte Gelder zu waschen. Eine besondere Verwundbarkeit ergibt sich, wenn solche Gesellschaften in Staaten angesiedelt sind, die nur bedingt mit den schweizerischen Strafverfolgungsbehörden kooperieren.

4.1.4 Finanzagenten

Ein häufiger Modus Operandi, um das Geld aus einem Betrug oder einem betrügerischen Missbrauch einer DVA zu waschen, ist der Einsatz von sogenannten Finanzagenten, auch *Money Mules* («Geldesel») genannt. Die Betrüger sind einfallsreich, wenn es darum geht, Gehilfen für die Weiterleitung der ergaunerten Gelder zu finden. Die meisten Personen werden mit einem verlockenden Stellenangebot als Finanzagent geködert, der angeblich für international tätige Unternehmen (oft im Bereich Immobilienhandel) den Zahlungsverkehr aus der Schweiz abwickeln soll. Weniger oft geben sich die Kriminellen als karitative Organisation aus, die Vertreter in der Schweiz suchen, um Spenden für notleidende Kinder in Krisengebiete zu transferieren.[105] In einigen Fällen treten die Betrüger auch auf Partnervermittlungs-Portalen oder Social-Network-Seiten als heiratswillige, osteuropäische Frauen auf und gaukeln Schweizer Männern eine Liebesbeziehung vor. Gewöhnlich versuchen die Betrüger in diesen Fällen zuerst, die Männer dazu zu bewegen, eigenes Geld für eine vermeintliche Reise der Partnerin in die Schweiz zu überweisen. Wenn sie dies nicht können oder wollen, geben die Betrüger vor, ein entfernter Verwandter könne die benötigte Summe aufbringen, der Finanzagent müsse das Geld jedoch von seinem Konto aus weiterleiten. Da die Geldtransferinstitute inzwischen vermehrt auf die Problematik sensibilisiert sind und in der Folge in vielen Fällen die Transaktionen verweigern, werden die Finanzagenten beauftragt, die Summe bar zu beziehen und mittels internationalen Paket- und Expressversandunternehmen zu verschicken. Die in Aussicht gestellte Kommission beträgt üblicherweise zwei bis zehn Prozent der zu überweisenden Summe. Durch diese Tätigkeiten erfüllen die Finanzagenten den objektiven Tatbestand der Geldwäscherei und riskieren ein Strafverfahren.

Die Summen, die über die Finanzagenten laufen, sind oft relativ gering, gewöhnlich weniger als 20’000 Franken. Sie machen aber mengenmässig einen grossen Teil der an MROS adressierten Verdachtsmeldungen aus und generieren somit einen erheblichen Arbeitsaufwand für

[104] KGGT (2017), op. cit.
[105] Bundesamt für Polizei fedpol (2011b), op. cit, S. 5.

die Strafverfolgungsbehörden. Des Weiteren zeigt die Auswertung von Entscheiden von Gerichten und Staatsanwaltschaften, dass die Finanzagenten unter Umständen wegen mangelndem Vorsatz freigesprochen werden. Gewisse Fälle werden zudem als geringfügige Vermögensdelikte angesehen, die keine Vortat zur Geldwäscherei bilden.[106]

Fallbeispiel Finanzagent
A wurde im Internet auf ein Stelleninserat der Immobilienfirma XY aus Grossbritannien aufmerksam, in dem Regionalverantwortliche gesucht wurden. Gemäss dem Arbeitsvertrag, den A per Mail erhielt, bestand ihre Aufgabe unter anderem darin, im Zusammenhang mit Immobiliengeschäften geleistete Zahlungen von Kunden auf ihrem Konto entgegenzunehmen und das Geld per Paket- und Expressversandunternehmen weiterzuleiten. Als Entlohnung durfte sie drei Prozent der überwiesenen Beträge behalten. Anfang 2015 veranlasste eine unbekannte Täterschaft mittels Malware-Attacke eine Überweisung von 7'630 Franken vom Konto eines Schweizer Ehepaares auf das Bankkonto von A. Wenig später wurde A zweimal von einer unbekannten Frau kontaktiert und angewiesen, die eingegangene Summe abzüglich der Kommission abzuheben und per Paket- und Expressversandunternehmen an eine ihr unbekannte Person in Moskau weiterzuleiten. Da die Überweisung an A jedoch von der Bank als mutmasslich betrügerisch erkannt und blockiert wurde, blieb es bei der versuchten Geldwäscherei. A wurde dafür per Strafbefehl mit einer unbedingten Geldstrafe von 30 Tagessätzen zu je 30 Franken bestraft.

4.1.5 Internationalisierung von betrügerischen Vortaten und deren Geldwäscherei

Sehr viele der Verfahren im Bereich der Wirtschaftskriminalität weisen einen internationalen Bezug auf. Durch das Internet können Kriminelle von fernen Ländern aus Betrüge in der Schweiz durchführen. Selbst wenn Täter und Opfer in der Schweiz sitzen, weisen manche Ermittlungen internationale Verbindungen auf, etwa wenn die betroffenen Server ausserhalb der Schweiz angesiedelt sind oder das inkriminierte Geld ins Ausland überwiesen wird. Grundsätzlich kann jeder Betrug oder Missbrauch einer DVA einen ausländischen Bezug haben. Betroffen sind aber vor allem Cyberbetrüge wie Phishing, Vorschussbetrüge, falsche internationale Überweisungsaufträge, falsche Hilfeleistung und Unterstützungsanfragen oder *Romance Scams* (Heiratsschwindel). Auch viele Anlage- oder Geldwechselbetrüge weisen Bezüge zum Ausland auf. Hinzu kommen Straftaten, die im Ausland begangen worden sind, und bei welchen sich zumindest ein Teil der Gelder in der Schweiz befindet, um über das schweizerische Finanzsystem gewaschen zu werden.

Die Täter arbeiten länderübergreifend, sehr schnell und mit wechselnden, falschen Identitäten. Die strafrechtliche Aufarbeitung solcher Fälle erfordert zumeist spezifische Kenntnisse im Bereich IT. Zudem ist der Ressourcenaufwand unverhältnismässig gross, da in diesem Bereich die jeweiligen Einzeldelikte punkto Anzahl Geschädigte und Schadensumme verhältnismässig klein sind, das heisst in der Regel im drei- bis höchstens vierstelligen Bereich. Obwohl Hinweise bestehen, dass eine Täterschaft in den meisten Fällen für eine ganze Reihe von Delikten verantwortlich ist, gelingt es kaum, diesen Nachweis zu erbringen. Nur in seltenen Fälle liefern die Einzeldelikte genügend Spuren, um von ihnen auf eine grössere Struktur zu schliessen.

Die Ermittler sind in Fällen mit internationalen Bezügen auf die internationale Rechtshilfe angewiesen, um die Taten aufklären zu können. Befragte Vertreter der Strafverfolgungsbehörden beschreiben die internationale Zusammenarbeit via internationale Rechtshilfe teilweise als zeitintensiv. Mehrheitlich können die benötigten Informationen aber dennoch beschafft werden. Den Erfahrungen der Strafverfolgungsbehörde zufolge ist es am erfolgversprechendsten, wenn die Rechtshilfeersuchen so kurz und konkret wie möglich formuliert werden. In der Praxis hat sich ebenfalls gezeigt, dass durch polizeiliche Abklärungen sowie den Informationsaustausch unter den Financial Intelligence Units (FIU) im Vorfeld von strafprozessualen Untersuchungen die Rechtshilfe entlastet und effizienter gestaltet werden kann. Zwar sind Informationen, die auf dem Wege der polizeilichen Zusammenarbeit, und somit nicht via Rechtshilfe,

[106] Innerhalb des Cyberboards (siehe 1.3) behandeln Staatsanwaltschaften und Polizeikorps regelmässig das Thema Finanzagenten.

gewonnen werden, nicht gerichtsverwendbar und dürfen auch nicht ohne Zustimmung der betroffenen FIU an andere Behörden weitergegeben werden. Gestützt auf diese Daten können aber dennoch gezielte Erhebungen der Staatsanwaltschaft auf dem Weg der Rechtshilfe erfolgen, die dann als Beweismittel in schweizerischen Verfahren in Anwendung des Rechtshilfegesetzes verwendet werden können. Einige Länder wie Deutschland oder Frankreich verfügen beispielsweise über zentrale Bankkontenregister. Diese enthalten keine Informationen über Kontostände oder Banktransaktionen, sondern lediglich Angaben darüber, ob eine Person über eine Bankkontoverbindung im entsprechenden Land verfügt, und mit welcher Bank. Auf europäischer Ebene sieht die EU-Richtlinie 2018/843 vor, dass die Mitgliedstaaten bis am 10. September 2020 zentrale automatische Mechanismen wie zentrale Register oder zentrale elektronische Datenabrufsysteme einrichten, die die zeitnahe Ermittlung aller Personen ermöglichen, die bei Kreditinstituten in ihrem Hoheitsgebiet Zahlungskonten und Bankkonten innehaben oder kontrollieren. Die in den genannten zentralen Mechanismen aufbewahrten Informationen müssen den nationalen zentralen Meldestellen und zuständigen Behörden zugänglich sein.[107]

4.1.6 Krypto-Assets

Das Risiko, das sich aus dem Einsatz von Krypto-Assets ergibt, kann aufgrund der wenigen bekannten Fälle nicht präzis beurteilt werden.[108] Die Tatsache, dass Transaktionen oft schnell, international und meistens auch ohne Finanzintermediär stattfinden, bildet aber eine erhebliche Verwundbarkeit. Es ist zudem ohne sogenannte *Private Key* kaum technisch möglich inkriminierte Vermögenswerte zu beschlagnahmen. Erschwerend kommt hinzu, dass dank sogenannter Mischdienste (auch *Mixer* oder *Tumbler* genannt) die Vermögenswerte stark vermischt bzw. auf mehrere Zieladressen aufgeteilt werden können, um deren kriminelle Herkunft zu verschleiern. Krypto-Assets bei Betrugsdelikten traten bislang vor allem bei Anlagebetrügen, unter anderem in Zusammenhang mit ICOs (*Exit Scams*), mit gewissen Schneeballsystemen und Ponzi-Schemen, sowie bei sogenannten *Phishing Scams*[109] und in manchen *Rip-Deal*-Fällen auf.

4.2 Verwundbarkeiten und Herausforderungen in Verbindung mit dem rechtlichen und institutionellen Dispositiv

Die Verwundbarkeiten in Verbindung mit dem institutionellen Dispositiv haben oft mit der rechtlichen Handhabung des Betrugs zu tun. Diese stellt für sich eine Herausforderung für die Strafverfolgungsbehörden dar. Dabei erweist sich der Straftatbestand des betrügerischen Missbrauchs einer DVA als weniger problematisch. Die Verwundbarkeiten sind vor allem auf folgende Elemente zurückzuführen: die Vielseitigkeit des Betrugs und dessen komplexe Tatbestandsmerkmale, die unterschiedlichen Verjährungsfristen von Vortat und Geldwäscherei, den Nachweis der Vortat, die Unterschiede zwischen dem Geldwäscherei- und Betrugsverfahren, die rechtzeitige Vermögensabschöpfung und nicht zuletzt das Unentdeckt bleiben der Straftat.

4.2.1 Vielseitigkeit des Betrugs

Die Gefährdungsanalyse hat gezeigt, dass ein Betrug oder ein betrügerischer Missbrauch einer DVA auf vielfältige Weise durchgeführt werden kann. Diese Vielfalt stellt eine Verwundbarkeit dar, da sie die Erkennung, die Analyse und letztlich auch die Strafverfolgung der Betrugsdelikte erschwert. So muss beispielsweise bei jedem neuen Betrugsphänomen die Frage gestellt werden, ob Arglist vorliegt.

Diese Diversität sticht ebenfalls aus den qualitativ ausgewerteten Verfahren heraus. Die Auswertung identifizierte verschiedene unterschiedliche Modi Operandi. Diese Vielfalt betrifft nicht nur die Art und Weise des kriminellen Handels, sondern auch die Verfahrensdauer oder den Schaden. So kann ein Verfahren beispielsweise bereits nach einem Monat wieder eingestellt,

[107] Art. 32a der EU-Richtlinie 2018/843 vom 30. Mai 2018.
[108] KGGT (2018b), op. cit.
[109] Eine Phishingvariante, wo das Opfer dazu verleitet wird, Informationen zu teilen, die den Betrügern Zugang zur Wallet und damit zum Private Key gewähren.

ein anderes jedoch erst nach mehr als zwölf Jahren nach Eröffnung abgeschlossen werden. Im Schnitt dauerten die Verfahren bei den untersuchten Justizentscheiden knapp drei Jahre. Punkto involvierte Vermögenswerte reicht die Spannweite von ein paar hundert Franken bis zu Beträgen im zweistelligen Millionenbereich.

Die anschliessenden Geldwäschereihandlungen nutzen vielfältige Modi Operandi, die auch in Verfahren im Zusammenhang mit anderen Vortaten beobachtet werden. In den untersuchten Verfahren wurde von den Tätern mehrheitlich versucht, die Spur des Geldes durch Verschiebungen über Konten im In- und Ausland zu verschleiern. Wie die MROS-Verdachtsmeldungen ebenfalls zeigen, wurde die Vortat in vielen Fällen im Ausland verübt. Die Beschuldigten liessen die Vermögenswerte in der Folge in die Schweiz fliessen. Nicht selten wurden die Gelder anschliessend wieder ins Ausland verschoben, teilweise zurück ins Herkunftsland, teilweise in andere Länder mit grösseren Finanzplätzen. Um die Identität der wirtschaftlich Berechtigten zu verschleiern, wurden die Transaktionen zudem in manchen Fällen von einer oder mehreren Gesellschaften getätigt, hinter denen die Täterschaft stand. Solche aufwändigen Konstrukte kommen allerdings eher bei grossen und komplexen Betrugsfällen vor. Um die Spur des Geldes zu unterbrechen, wurden Vermögenswerte ausserdem auch bar bezogen und anschliessend via Geldtransferinstitut ins Ausland transferiert. Dieser Modus Operandi konnte insbesondere im Zusammenhang mit Finanzagenten beobachtet werden. Die Betrüger gaben die ergaunerten Gelder auch häufig für ihren mitunter aufwändigen Lebensstil oder für die Begleichung von Schulden aus. Bei Delikten wie dem *Rip-Deal* oder dem Enkeltrickbetrug wird das inkriminierte Geld vor allem in bar über die Grenze gebracht.

Vielfältig kann auch die Anzahl der echten Konkurrenzen der verschiedenen Delikte sein. Vor allem bei grösseren Verfahren im Bereich der Wirtschaftskriminalität kommen in der Regel mehrere Gesetzesartikel zur Anwendung. Neben Betrug spielen oft Veruntreuung, ungetreue Geschäftsbesorgung, betrügerischer Missbrauch einer DVA und Urkundenfälschung, seltener auch betrügerischer Konkurs, eine Rolle. Da der Nachweis eines Betrugsdelikts aufgrund seines kaskadenartigen Aufbaus relativ aufwändig ist, konzentrieren sich die Strafverfolgungsbehörden bei ihren Ermittlungen nicht selten zuerst auf andere Delikte. Um in einem Verfahren die verfügbaren Ressourcen so effizient wie möglich einzusetzen, kann es in gewissen Fällen sogar Sinn machen, den Fokus des Verfahrens auf das bereits erkannte Delikt zu legen und den Vorwurf des Betrugs fallen zu lassen, sofern die Strafandrohung die gleiche ist. Es ist daher wahrscheinlich, dass ein Teil der Verdachtsmeldungen an MROS, in denen Betrug als Vortat vermutet wird, letztlich in ein Verfahren wegen Veruntreuung oder ungetreuer Geschäftsbesorgung mündet. Gemäss Aussagen von Experten aus der Strafverfolgung sollte weniger von Betrügern als allgemein von Wirtschaftsdelinquenten gesprochen werden, da dieser Begriff das Phänomen besser trifft.

Der Facettenreichtum der Betrugsdelikte in der Schweiz wird nur teilweise erfasst, so dass die einzelnen Betrugsphänomene nur ansatzweise analysiert werden können. Bezüglich Internetkriminalität, einschliesslich viele der oben erwähnten betrügerischen Phänomene, sollte die PKS allerdings ab kommendem Jahr verbesserte Auswertungsmöglichkeiten bieten.[110] Die Urteilstatistik ist ebenfalls nur auf die betroffenen Gesetzesartikeln beschränkt. Die fedpol-internen Verdachtsmeldungen (an MROS und zur Internetkriminalität) bieten mehr Analysemöglichkeiten, sind aber zur Einschätzung des Ausmasses des Phänomens nur sehr bedingt tauglich. Hier könnten Opferbefragungen weiterhelfen; diese haben bislang aber nur Teilaspekte der Betrugsdelikte abgedeckt.

4.2.2 Komplexität der Tatbestandsmerkmale des Betrugs

Als Straftatbestand weist der Betrug eine gewisse Komplexität auf: «Die Grenzziehung zwischen straflosem und strafbarem Verhalten ist beim Betrug mit empfindlichen Unsicherheiten

[110] Ein neues Schema zur Erfassung der Cyberkriminalität in der PKS, darunter auch sogenannte Cyberbetrüge, sollte ab 2019 verfügbar sein. Siehe Bundesamt für Statistik (2019), op. cit., S. 9.

belastet, die sich insb. bei der Täuschung und beim Schaden bemerkbar machen.»[111] So kann ein Betrug beispielsweise nur dann strafrechtlich relevant sein, wenn seine Arglist bejaht wird.

Den Schweizer Strafverfolgungsbehörden fällt es manchmal schwer, im Rahmen ihrer Strafverfahren den Nachweis der Arglist als Tatbestandsmerkmal des Betrugs zu erbringen.

In Fällen von Geldwäscherei mit einem im Ausland begangenen Betrug als Vortat muss nämlich Arglist nachgewiesen werden können, damit der Betrugsbegriff nach Schweizer Recht erfüllt ist. Diese Voraussetzung ist jedoch nach ausländischem Recht zuweilen nicht gegeben.

In einigen Fällen führte die fehlende Nachweisbarkeit der Arglist als Tatbestandsmerkmal eines im Ausland begangenen Betrugs zur Einstellung der Strafverfahren wegen Geldwäscherei, weil dadurch die Vortat fehlte.

Beispielsweise hatte das Bundesstrafgericht in seinem Entscheid vom 24. November 2010 (SK.2010.9) die Begehung eines Betrugs als Vortat zu einem Fall von Geldwäscherei verneint, weil das russische Recht, d.h. das Land, in dem der Betrug mutmasslich begangen worden war, den Betrugsbegriff breiter fasst als das Schweizer Recht, und die Arglist nicht als Tatbestandsmerkmal voraussetzt.

Auch bei Handlungen, die in der Schweiz begangen wurden, stellt das Element der Arglist für die Strafverfolgungsbehörden Herausforderungen dar. So gibt es immer wieder Fälle, die wegen mangelnder Arglist nicht zu einer Verurteilung führen. Als Beispiel kann hier das Verfahren gegen einen angeblichen Hellseher genannt werden: Er gab an, die Lottozahlen vorauszusehen, worauf ihm rund 700 Geschädigte eine Gebühr von 65 Franken bezahlten, um die Zahlen zu erfahren. Da das Kriterium der Arglist nicht gegeben war, entschied die zuständige Staatsanwaltschaft das Verfahren einzustellen Besonders bei geringeren Summen muss ein Opfer abwägen, ob es sich lohnt, eine Anzeige zu erstatten und sich auf ein Verfahren einzulassen, bei dem unklar ist, ob die Arglist letztendlich bejaht wird.

Andere Tatbestandsmerkmale des Betrugs können ebenfalls zu Beweisschwierigkeiten führen. Bei einer hohen Anzahl an Geschädigten, einer Vielzahl an Konten und Transaktionen sowie bei einer zumindest teilweisen Auszahlung fälliger Renditen gestaltet sich die Bezifferung des Schadens mitunter als schwierig. Zudem muss gemäss dem Prinzip der Stoffgleichheit[112] der Schaden (= Vermögensnachteil) der Bereicherung (= Vermögensvorteil) entsprechen. Das heisst, die vom Täter für sich oder für einen Dritten angestrebte Bereicherung muss die Kehrseite des beim Opfer eingetretenen Schadens sein.[113]

Auch die Kausalität der Tatbestandsmerkmale kann beim Betrug ein Problem sein: In einigen Fällen nehmen die Geschädigten eine Vermögensdisposition vor, ohne dass zuvor eine Täuschung erfolgte. Die Täuschung erfolgt dann erst bei einer verlangten Rückzahlung oder beim Anspruch auf Renditen. Bei einer solchen Faktenlage ist der Tatbestand des Betrugs nicht erfüllt, da die Vermögensverfügung eine unmittelbare Folge des Irrtums sein muss.[114]

Letztlich zeigen die ausgewerteten Urteile auch auf, dass sowohl beim Betrug als auch bei der Geldwäscherei (und wohl auch in anderen Bereichen der Wirtschaftskriminalität), der Nachweis des subjektiven Tatbestands eine Herausforderung darstellt. Betrüger handeln nicht immer genau nach einer im Voraus definierten Strategie, sondern agieren manchmal eher spontan. Aus diesem Grund ist es teilweise schwierig zu beurteilen, ob bei einem Betrug von Anfang an eine kriminelle Absicht im Vordergrund stand. So kann es beispielsweise vorkommen, dass ein Anlagebetrüger eine gewisse Zeit lang tatsächlich an seine Investitionsstrategie geglaubt hat. Dies trifft insbesondere für allfällige Mittäter zu, die typischerweise nur beschränkten Zugang zu wichtigen Informationen hatten. In den meisten Fällen kann ein routinierter Strafverfolger durch die Ermittlung von Wissenselementen beim Beschuldigten einen Moment in den

[111] Maeder/Niggli (2009), op. cit., S. 3093.
[112] Arzt, Gunther (2007): *Art. 146*, in: Niggli, Marcel Alexander/Wiprächtiger, Hans (Hrsg.): Strafrecht II, Art. 111–392 StGB. Basler Kommentar, 2. Aufl., Basel 2007, S. 551.
[113] Ibd.
[114] Ibd., S. 540.

Handlungen festmachen, an dem dieser, auch wenn er an seine Strategie geglaubt hat, die Notbremse hätte ziehen müssen. Hat er dies nicht getan, kann man für gewöhnlich von krimineller Absicht ausgehen.

Aufgrund dieser Komplexitäten ist das Ergebnis eines Betrugsverfahrens grundsätzlich mit einer höheren Unsicherheit verbunden als bei anderen Straftaten (wie z.B. bei einem Diebstahl). Dies führt somit zu einer gewissen Verwundbarkeit, da mutmasslich nicht jedes Opfer sich auf das Prozessrisiko einlässt, insbesondere, wenn nur geringe Summen im Spiel sind und ein Reputationsrisiko besteht.

4.2.3 Unterschiedliche Verjährungsfristen zwischen Vortat und einfacher Geldwäscherei

Manche Betrugsverfahren nehmen nicht nur wegen den internationalen Rechtshilfeverfahren viel Zeit in Anspruch, sondern auch wegen der Anzahl der involvierten Personen oder wegen der allgemeinen Komplexität des Falles.

In diesem Kontext erweisen sich ausserdem die erweiterten Teilnahmerechte in der aktuellen Strafprozessordnung als gewaltige Herausforderung. So steht unter anderem allen zur Einlegung eines Rechtsmittels legitimierten Parteien das Recht zu, bei Beweiserhebungen durch die Staatsanwaltschaft und die Gerichte anwesend zu sein und den einvernommenen Personen Fragen zu stellen[115]. Bei grossen Betrugsverfahren mit mehreren hundert Geschädigten ist dies schon rein logistisch problematisch.. Zudem, und wohl noch bedeutender, wird dadurch auch Mittätern erlaubt, bei der Einvernahme ihrer Komplizen anwesend zu sein. Ein aktuelles Projekt zur Teilrevision der StPO sieht aber vor, diese Teilnahmerechte einzuschränken.[116]

Die unterschiedlichen Verjährungsfristen zwischen Vortat – 15 Jahre für den Betrug und den betrügerischen Missbrauch einer DVA – und einfache Geldwäscherei - zehn Jahre - können manchmal zu Situationen führen, wo die durch das erstinstanzliche Urteil bestätigte Vortat erst vorliegt, nachdem die Verjährungsfrist für die Geldwäscherei schon abgelaufen ist. Sollten der Betrüger und der Geldwäscher unterschiedliche Personen sein, könnte letztere in einer solchen Situation ungeschoren davonkommen. Ein solches Szenario betrifft allerdings besonders komplexe und nicht allzu häufig vorkommende Fälle, wo zudem keine qualifizierte Geldwäscherei vorliegt.

Fallbeispiel Behring

Ab 1994 baute der Basler Financier Dieter Behring ein Anlagesystem auf, welches sich angeblich auf ein von ihm entwickeltes EDV-Systems stützte, mit dem er den «genetischen Code der Börse» geknackt haben wollte. In Wahrheit wurden nur die wenigsten Kundengelder angelegt, und meist zu bescheidenen Erträgen oder gar mit Verlusten. Vielmehr nutzte Behring die Einnahmen von den neu angeworbenen Kunden, um die Erträge des schon investierten Kapitals auszuzahlen und um sich zu bereichern. Dieses auf über 800 Millionen Franken basierende Umlagesystem (auch Ponzi-Schema genannt) platzte im Herbst 2004. Im Juni 2004 informierte MROS die Bundesanwaltschaft, dass verdächtige Vorgänge auf Konten mit Bezug zu Behring festgestellt wurden. Kurze Zeit später eröffnete die Bundesanwaltschaft ein gerichtspolizeiliches Verfahren gegen Behring und eine unbekannte Täterschaft. Das erstinstanzliche Strafverfahren dauerte zwölf Jahre: Am 30. September 2016 wurde Behring vom Bundesstrafgericht zu einer Freiheitsstrafe von fünf Jahren und sechs Monaten wegen gewerbsmässigen Betrugs zu Lasten von rund 2'000 Geschädigten verurteilt. Am 7. August 2018 bestätigte das Bundesgericht im Strafpunkt das erstinstanzliche Urteil. Das Verfahren hinsichtlich der Geldwäscherei wurde aufgrund der Verjährung eingestellt; qualifizierte Geldwäschereihandlungen, die eine längere Verjährungsfrist gehabt hätten, verneinte das Gericht, da die Gewerbsmässigkeit nur bei der Vortat vorliege und nicht bei der anschliessenden Geldwäscherei. Behring verstarb im Frühjahr 2019.

[115] Art. 147 StPO.
[116] Bundesrat (2019): Strafprozessordnung soll praxistauglicher werden. 28.08.2019. https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-76205.html.

4.2.4 Nachweis der Vortat

Der Nachweis der Vortat ist nicht nur problematisch, wenn diese gerichtlich nach der Verjährung der anschliessenden Geldwäschereihandlung vorliegt. Er stellt insbesondere bei einem im Ausland begangenen Betrug oder einem betrügerischen Missbrauch einer DVA eine grosse Hürde dar. Auch in der Schweiz kann es unter Umständen schwierig sein, von einer verdächtigen Finanztransaktion auf eine – für den Straftatbestand der Geldwäscherei notwendige – Vortat zu schliessen. Bei den Verfahren, die für diesen Bericht ausgewertet wurden, erfolgten im Übrigen die meisten Einstellungen, weil die Vortat, aus welcher die Vermögenswerte herrühren, nicht nachgewiesen werden konnte.[117] In anderen Fällen kam das Gericht zum Schluss, dass keine Vereitelungshandlung vorlag. Eine Einzahlung auf das eigene Bankkonto im Inland beispielsweise stellt in der Regel keine Vereitelungshandlung dar.[118]

4.2.5 Unterschiede zwischen Geldwäscherei- und Betrugsverfahren

Verfahren, die durch eine Geldwäschereimeldung mit Betrug als vermutete Vortat ausgelöst werden, lassen sich nur bedingt mit Verfahren vergleichen, die in erster Linie wegen Betrug geführt werden. Die durch eine Geldwäschereiverdachtsmeldung ausgelösten Verfahren betreffen oft ein Betrugsdelikt, das im Ausland stattgefunden hat. In diesen Fällen gelangen die Gelder dann auf unterschiedliche Art und Weise in die Schweiz und der hiesige Finanzplatz wird somit mutmasslich zu Geldwäschereizwecken missbraucht. Meist werden Schweizer Finanzintermediäre durch Presseberichte oder spezialisierte Datenbanken auf die Verwicklung eines Kunden in ein solches Delikt aufmerksam und erstatten in der Folge eine Meldung an MROS. Die zuständigen Strafverfolgungsbehörden versuchen dann abzuklären, ob die in der Schweiz deponierten Vermögenswerte tatsächlich aus dem im Ausland begangenen Delikt stammen.

Im Gegensatz dazu werden auf Betrug ausgerichtete Verfahren, insbesondere in den Kantonen, oft nicht wegen einer Geldwäschereiverdachtsmeldung, sondern aus anderen Gründen ausgelöst. In der Mehrheit der Fälle dürften die Strafverfolgungsbehörden aufgrund von Anzeigen durch die Geschädigten tätig werden. Insbesondere bei den Strafverfolgungsbehörden des Bundes werden Verfahren immer wieder auf der Basis von Rechtshilfeersuchen aus anderen Staaten eröffnet. Wenn im Zuge von Betrugsermittlungen Transaktionen ins Ausland oder andere Vereitelungshandlungen aufgedeckt werden, dokumentieren die Ermittler diese für eine Anklage wegen Geldwäscherei. Darüber hinaus hat die Aufdeckung von Geldwäschereihandlungen in Betrugsverfahren aber lediglich eine untergeordnete Priorität, da das Strafmass durch eine zusätzliche Verurteilung wegen Geldwäscherei nur marginal erhöht würde und sich die aufwändigen Geldwäschereiermittlungen daher aus verfahrensökonomischen Gründen nicht lohnen. Es ist also davon auszugehen, dass ein grosser Anteil an Geldwäschereihandlungen mit Betrugsdelikten als Vortat nicht untersucht wird und folglich eine hohe Dunkelziffer besteht. In anderen Bereichen dürfte dies ähnlich sein: Auch beim Handel mit Betäubungsmitteln oder bei Diebstählen wird nicht systematisch zusätzlich wegen Geldwäscherei ermittelt, da sich auch hier der zu betreibende Aufwand in den meisten Fällen nicht rechtfertigt. Im Gegensatz zu den strafrechtlichen Folgen ist aber die Aufdeckung von Geldwäschereihandlungen bezogen auf Vermögenssicherung bzw. Vermögenseinziehung von grosser Bedeutung. Durch die Aufschlüsselung von Transaktionen, Barbezügen, Investitionen und weiteren Vereitelungshandlungen können die Ermittler nachvollziehen, wohin die betrügerisch erlangten Vermögenswerte geflossen sind. Im Idealfall werden sie in der Folge blockiert und am Ende des Verfahrens eingezogen.

4.2.6 Rechtzeitige Vermögensabschöpfung

Betrüger erbeuten durch Betrugsdelikte in manchen Fällen Millionen. Diese Vermögenswerte werden vom Gericht aufgrund des Prinzips, wonach sich Verbrechen nicht lohnen dürfen, eingezogen. Die Vermögensabschöpfung stellt aber eine Herausforderung dar. Ausführliche

[117] Bundesamt für Polizei fedpol (2014), op. cit.
[118] Vgl. BGE 124 IV 274, E 4., S. 279-280.

Nachforschungen zu vorhandenen Vermögenswerten im Umfeld des Täters müssen idealerweise in einem frühen Verfahrensstadium vorgenommen werden. Solche Abklärungen können das eigentliche Verfahren aber verzögern und werden daher noch nicht immer systematisch vorgenommen. Zudem ist die akribische Erfassung und Prüfung der Ansprüche der Geschädigten sehr aufwändig und ressourcenintensiv. Am Anfang der Verfahren stehen die Ermittler ausserdem nicht selten vor einem undurchsichtigen Betrugskonstrukt; Geldflüsse können oft erst nach Monaten oder Jahren nachvollzogen werden. Surrogate, die beispielsweise nach der Mischung von legalen und illegalen Vermögenswerten entstanden sind, erschweren die Einziehung zusätzlich. Zudem schieben die Betrüger die Schuld für den Zusammenbruch des Systems typischerweise auf die Strafverfolgungsbehörden und beteuern, dass die nächsten Renditen ohne die Einmischung der Polizei und Staatsanwaltschaft demnächst ausbezahlt worden wären. Aus Ärger und Unverständnis gegenüber den Strafverfolgungsbehörden melden sich in der Folge nur wenige Geschädigte, wodurch der Polizei wichtige Informationen entgehen. Nicht selten zeigen sich die Geschädigten überdies unkooperativ, weil sie nicht versteuerte Vermögenswerte investiert hatten.[119]

4.2.7 Unentdeckt bleiben der Straftat

Die Strafbehörden sind verpflichtet, im Rahmen ihrer Zuständigkeit, ein Verfahren einzuleiten und durchzuführen, wenn ihnen Straftaten oder auf Straftaten hinweisende Verdachtsgründe bekannt werden.[120] Problematisch ist aber, dass insbesondere bei Waren- und Lebensmittelbetrug, punktuell auch bei anderen Phänomenen, der Betrug oft unbemerkt bleibt. Der Endkunde, der eine absichtlich gepanschte, aber als extra natives verkauftes Olivenöl erwirbt, wird vermutlich nie erfahren, dass er betrogen wurde. Komplizierte Geldwäschereihandlungen sind für den Täter somit kaum noch nötig, da nicht einmal die Vortat entdeckt wird. Das heisst aber nicht, dass solche Vermögenswerte nicht gewaschen werden. Im Gegenteil dürfte aufgrund der zahlreichen im Lebensmittelbereich vermuteten Betrugsfälle besonders viel Geld gewaschen werden. Allerdings werden solche Geldwäschereihandlungen in der Regel nicht aufgedeckt, da die Gelder dem Anschein nach legal sind. Dieses Unentdeckt bleiben gewisser Betrugsarten bildet somit eine grosse Verwundbarkeit.

5 Bewertung des Risikos ausgehend vom Betrug und dem Missbrauch einer Datenverarbeitungsanlage als Vortat zur Geldwäscherei

5.1 Folgen für die Schweiz

Die Folgen von Betrugsdelikten als Vortat zur Geldwäscherei sind schwierig abzuschätzen, scheinen sich aber im Grossen und Ganzen dank eines grundsätzlich wirksamen Abwehr- und Bekämpfungsdispositivs nicht auf die Gesellschaft, den Finanzsektor oder Dienstleistungsbereiche auszuwirken. Zwar können die finanziellen Schäden für einzelne Opfer oder auch den Staat erheblich sein (beispielsweise bei einem Anlagebetrug), die Möglichkeiten der Vermögensabschöpfung und Ersatzforderungen können diese Schäden jedoch teilweise mindern. Präventive Wirkung kann auch die Geldwäschereigesetzgebung entfalten, indem sie es ermöglicht, gewisse verdächtige Zahlungen zu stoppen.

5.2 Schlussbewertung des Geldwäschereirisikos

Die Risikoeinschätzung betreffend Betrugsdelikte als Vortat zur Geldwäscherei hat sich in den letzten Jahren nicht wesentlich verändert. Wie diese sich in näherer Zukunft entwickeln wird, hängt wesentlich von der Entwicklung der Internetkriminalität ab. Die aktuelle Faktenlage ist allerdings noch zu dürftig, um eine genaue Prognose abgeben zu können. Dafür sind weitere

[119] Bundesamt für Polizei fedpol (2011a): Jahresbericht 2010, S. 18. https://www.fedpol.admin.ch/dam/data/fedpol/publiservice/publikationen/berichte/jabe/jabe-2010-d.pdf.
[120] Art. 7 StPO.

wissenschaftlich durchgeführte Studien, insbesondere auf Betrugsdelikte fokussierte Opferbefragungen, nötig. Betrüge können im Einzelfall mit erheblichen finanziellen oder psychischen Konsequenzen verbunden sein. Das Ausmass und die Wirkung solcher Straftaten stellen in ihrer Gesamtheit aber bislang keine systemrelevante Gefahr für die Schweiz dar. Dafür spricht auch die Tatsache, dass die Deliktsumme in der Mehrheit der Fälle verhältnismässig bescheiden ist, in der Regel unter 10'000 Franken. Der Bericht zeigt dennoch, dass gewisse Betrüge durchaus ein grosses Ausmass annehmen und unter besonderen Umständen weitreichende Konsequenzen nach sich ziehen können. Allerdings stellt in solchen Fällen vor allem die Vortat und nicht unbedingt die nachfolgende Geldwäschereihandlung die grösste Bedrohung dar. Wahrscheinlicher ist das Risiko, dass der Schweizer Finanzplatz für die Geldwäscherei von Vermögenswerten missbraucht werden könnte, welche aus im Ausland begangenen Betrügen stammen und dort systemrelevant sein können.

Theoretisch dürften betrügerische Missbräuche einer DVA und Betrüge – sofern diese nicht als geringfüge Vermögensdelikte gelten – fast immer eine oder mehrere Geldwäschereihandlungen zur Folge haben. Es ist anzunehmen, dass die meisten Täter das Geld nicht ausschliesslich auf ihrem eigenen Konto horten, sondern in einer Art und Weise verwenden, die als Geldwäscherei eingestuft werden kann. Zwar bieten Informations- und Kommunikationstechnologien neue Betrugsopportunitäten, die teilweise mit einer vermuteten Verlagerung von der «klassischen» hin zur Internetkriminalität einhergehen. Dennoch hat sich das Geldwäschereirisiko in den letzten Jahren nicht wesentlich verändert; es stellt wie die Vortaten Betrug und betrügerischer Missbrauch einer DVA weiterhin keine systemrelevante Gefahr dar.

Geldwäschereihandlungen geraten aber mit der Internetkriminalität stärker in den Fokus der Strafverfolgungsbehörden. Betrugsdelikte, die mithilfe des Internets begangen werden, erfordern meistens Geldverschiebungen über Finanzintermediäre. Die Illegalität solcher Transaktionen dürfte mit einem effizienten Kontrollsystem oft erkennbar sein. Das grösste Geldwäschereirisiko entsteht da, wo die zu waschenden Vermögenswerte nicht rechtzeitig erkannt, nachverfolgt und eingezogen werden können. Insbesondere erweisen sich die zahlreichen Fälle als problematisch, in welchen verhältnismässig geringe Summen aus dem oder im Ausland gewaschen werden. Nicht selten kommen dabei Finanzagenten zum Einsatz. Kleinere Transaktionen sind oft schwieriger zu entdecken, da sie nicht so auffällig sind. Ausserdem generieren sie, wenn sie erkannt werden, verhältnismässig viel Aufwand für die ermittelnde Strafverfolgungsbehörde. Die vergleichsweise grössten Geldwäschereirisiken dürften sich somit vor allem aus den zumeist mithilfe des Internets durchgeführten Betrugsarten ergeben: i) Betrug auf Verkaufs- und Immobilienportalen, ii) Phishing zum Zweck eines Missbrauchs einer DVA, iii) Anlagebetrüge und iv) falsche internationale Überweisungsaufträge. Ebenfalls risikobehaftet erscheint der v) Konkursbetrug und der vi) Lebensmittelbetrug. Die zwei ersten Phänomene bilden, insbesondere aufgrund deren Ausmasses und gesamten Schadensumme, ein erhöhtes Geldwäschereirisiko, wobei viele, wenn auch verhältnismässig kleine Summen dadurch in der Schweiz oder im Ausland gewaschen werden. Anlagebetrüge und falsche internationale Überweisungsaufträge sind wiederum aufgrund der durchschnittlich grossen finanziellen Folgen für die Betroffenen und den damit verbundenen hohen zu waschenden Vermögenswerten risikobehaftet. Der Konkursbetrug lag aufgrund der weiteren tangierten Sondertatbestände nicht im Hauptfokus dieses Berichtes; viele Elemente, vor allem die hohe geschätzte Schadensumme, indizieren jedoch, dass diese Delikte ebenfalls ein Geldwäschereirisiko für die Schweiz darstellen. Letztlich ist der Lebensmittelbetrug zu nennen, dessen Ausmass gemäss verschiedenen Indikatoren gross ist, der aber gemeinhin unterschätzt wird, weil er meist unentdeckt bleibt. Lebensmittelbetrug ist zudem eine der wenigen Betrugsarten, die im schlimmsten Fall auch ein Gesundheitsrisiko darstellen können.

Die Risikobewertung für die einzelnen betrügerischen Phänomene wird in der nachfolgenden Tabelle zusammengefasst:

Risikobewertung		
Gefährdung *(threat)*	Verwundbarkeit *(vulnerability)*	Folgen *(consequence)*
Betrug bei Firmenkonkursen	· mangelnde Liquiditätsprüfung durch Gläubiger bei Leasing- und Bestellungen · bisher kaum systematisches Vorgehen bei Prävention und Repression · mangelnde Sensibilisierung der involvierten Stellen (Konkursamt, Notare etc.)	· beträchtliche finanzielle Schäden (insbesondere für das Gemeinwesen)
MwSt-Karussellbetrug	· schwierig aufzudecken · nur schwer als Betrug erkennbar	· hoher Schaden für das Gemeinwesen
Betrug im Beschaffungswesen	· schwierig aufzudecken	· hoher Schaden für das Gemeinwesen
Phishing	· Massenversand · geringer technischer Aufwand für Datenbeschaffung · Täter im Ausland · Rechtshilfe nicht immer einfach · hohe technische Komplexität der Delikte	· Vertrauensverlust in Online-Geschäftsverkehr · Täter können oft nicht bestraft werden
Falsche internationale Überweisungsaufträge	· wenig geschützte IT-Infrastruktur · rudimentäres internes Kontrollsystem · Täter im Ausland · Rechtshilfe nicht ganz einfach · Einsatz von informellen Überweisungssystemen vermutet	· hohe finanzielle Schäden für Unternehmer · Täter können oft nicht bestraft werden
Kreditbetrug	· geringer Aufwand für Täter · oft standardisierter Ablauf bei Kreditvergabe	· hoher Schaden für Kreditgeber
Versicherungsbetrug	· oft standardisierter Ablauf bei Schadenmeldung	· finanzielle Schäden sehr unterschiedlich
Lebensmittelbetrug	· findet oft unbemerkt statt · komplexe Lieferketten mit vielen Akteuren · oft internationaler Bezug	· finanzielle Schäden sehr unterschiedlich · in Extremfällen gesundheitsgefährdend

Betrug auf Verkaufs- und Immobilienportale	· geringer technischer Aufwand · Unterbruch *Paper Trail* · kleine Beträge · unverhältnismässiger Ressourceneinsatz für Aufklärung notwendig	· oft nur geringe finanzielle Schäden bei einem Opfer · Vertrauensverlust in Händler · hohe Wiederholungsrate
Anlagebetrug	· komplexe Sachverhalte und «Produkte» · z.T. schwierige Überprüfbarkeit durch Anleger · grosse Verfahren mit einer Vielzahl an Geschädigten	· Vertrauensverlust in Vermögensanlagen · sehr hohe Schäden bei Anlegern
Falsche Unterstützungsanfrage	· Täter im Ausland und mit falschen Identitäten · Rechtshilfe nicht einfach · kein *Paper Trail*, wenn es um Bargeld geht	· Opfer verzichten auf Anzeige wegen Scham · nur die Geldabholer werden gefasst; Drahtzieher oft unbestraft
Falsche Hilfeleistung	· Täter im Ausland und unter falschen Identitäten · meistens kein *Paper Trail*, da es oft um Bargeld geht	· teilweise für Privatpersonen hohe finanzielle Schäden · nur die Geldabholer werden gefasst; Drahtzieher oft unbestraft
Vorschussbetrug	· Massenversand · Unterbruch *Paper Trail* · kleine Beträge · Täter im Ausland und unter falschen Identitäten · Rechtshilfe nicht immer einfach	· oft verhältnismässig geringe finanzielle Schäden bei einem Opfer · teilweise aber Verschuldung im sozialen Umfeld · Gefahr psychischer Abhängigkeit zu Tätern · Täter können oft nicht bestraft werden
Geldwechselbetrug	· meistens kein *Paper Trail*, da es oft um Bargeldgeschäfte geht	· hoher Schaden beim *Rip-Deal* · oft verhältnismässig geringe finanzielle Schäden bei den anderen Varianten
Heiratsschwindel / *Romance Scam*	· nutzen Einsamkeit der Opfer aus · Täter im Ausland und unter falschen Identitäten · Rechtshilfe nicht immer einfach	· finanzielle Schäden sehr unterschiedlich · psychische Schäden bei den Opfern · Täter können oft nicht bestraft werden
Darlehensbetrug	· kleine Beträge	· oft verhältnismässig geringe finanzielle Schäden bei einem Opfer

Betrug beim Warenerheben oder Warenverkauf	· findet z.T. unbemerkt statt · oft internationaler Bezug	· finanzielle Schäden sehr unterschiedlich

5.3 Empfehlungen

Aus den Feststellungen dieses Berichts ergeben sich die folgenden Handlungsempfehlungen zuhanden der KGGT:

- **Faktenlage verbessern:** Dieser Bericht zeigt, dass die aktuellen Daten das Phänomen der Betrugsdelikte nur teilweise erfassen. Auch wenn die Komplexität des Betrugs – und in geringerem Masse des Missbrauchs einer DVA – wohl nie vollständig erfasst werden kann, sind Verbesserungen möglich. Regelmässige unabhängige und wissenschaftlich fundierte Opferbefragungen, die sich spezifisch den Betrugsdelikten widmen und sowohl juristische als auch natürliche Personen erfassen, würden einen besseren Überblick erlauben. Bei bereits bestehenden Statistiken, insbesondere der PKS, sollte geprüft werden, wie die Vielfalt des Betrugs besser erfasst werden kann.[121] Unter anderem wäre denkbar, alle nicht online durchgeführten Betrugsarten systematisch in der PKS nach deren Form zu unterscheiden.[122] Prüfenswert wäre zudem die Frage, ob und inwiefern die Schadensumme und die Vortat bei Geldwäschereistraftaten erfasst werden könnten.
- **Sensibilisierung fortsetzen:** Die Schweiz verfügt bereits heute über gut ausgebaute und professionelle Präventionsmechanismen (vgl. Kapitel 1.2). Betrüger finden aber immer neue Wege, um ihre Opfer zu täuschen. Es ist daher essentiell, dass Akteure im Präventionsbereich stets über die neusten Modi Operandi informiert sind und ihre Hinweise an die Bevölkerung laufend anpassen und vervollständigen. Im Bereich der Internetkriminalität sieht die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018-2022 bereits eine «Früherkennung von Trends und Technologien und Wissensaufbau» sowie einen Ausbau der Sensibilisierung vor.[123] Eine Verstärkung der Sensibilisierung sollte indes auch betreffend nicht online durchgeführte Betrugsarten geprüft werden.

[121] Ein neues Schema zur Erfassung der Cyberkriminalität in der PKS, welches sich u.a. auf den von fedpol entwickelte Phänomenkatalog abstützt, dürfte ab dem Berichtsjahr 2019 verfügbar sein.
[122] Z.B. anhand der aktuellen Betrugskategorien: Betrug (unspezifiziert), Darlehensbetrug, Kreditbetrug, Vorschussbetrug, Geldwechselbetrug, Betrug beim Warenerheben/Verkauf, Betrug beim Fahrzeugerheben/Verkauf, Versicherungsbetrug, Heiratsbetrug, Scheckbetrug, Spielbetrug, Hotelbetrug.
[123] Bundesrat (2018): Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022. https://www.isb.admin.ch/dam/isb/de/dokumente/ikt-vorgaben/strategien/ncs/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_DE.pdf.download.pdf/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_DE.pdf.

6 Literaturverzeichnis

Ackermann, Jürg-Beat (2019): Das Submissionskartell – Sicht des Strafrechts. Luzern 18.02.2019.
https://www.unilu.ch/fileadmin/fakultaeten/rf/diebold/Tagung_Submissionskartell/Ackermann_Submissionskartell_Strafrecht.pdf [04.03.2020]

Arzt, Gunther (2007): *Art. 146*, in: Niggli, Marcel Alexander / Wiprächtiger, Hans (Hrsg.): Strafrecht II, Art. 111–392 StGB. Basler Kommentar, 2. Aufl., 2007, S. 513-558

Balzli, Tina (2018): *Art. 3 Abs. 1 lit. r*, in: Heizmann, Reto / Loacker, Leander D. (Hrsg.): UWG Bundesgesetz gegen den unlauteren Wettbewerb. Kommentar. Zürich 2018 S. 700-726

Beaudet-Labrecque, Olivier / Brunoni, Luca / Augsburger-Bucheli, Isabelle (2018a): Finanzieller Missbrauch. Nationale Studie zur Untersuchung der Betrugsarten in der Altersgruppe 55+. Pro Senectute Schweiz (Hrsg.). Zürich 2018.
https://www.prosenectute.ch/dam/jcr:e0a731a4-ab86-4810-b10c-e4f532374ad4/Finanzieller-Missbrauch-Studienbericht-01.10.2018.pdf [04.03.2020]

Beaudet-Labrecque, Olivier / Brunoni, Luca / Augsburger-Bucheli, Isabelle (2018b): «Finanzieller Missbrauch» - häufigste Betrugsarten in der Schweiz. Pro Senectute Schweiz (Hrsg.). Zürich 2018.
https://www.prosenectute.ch/dam/jcr:7d5c59ff-5b6b-468c-8666-3a6d21abe729/Finanzieller-Missbrauch-haeufigste-Betrugsformen-in-der-Schweiz-01.10.2018.pdf [04.03.2020]

Biberstein, Lorenz / Killias, Martin / Walser, Severin / Iadanza, Sandro / Pfammatter, Andrea (2016): Studie zur Kriminalität und Opfererfahrungen der Schweizer Bevölkerung. Analysen im Rahmen der schweizerischen Sicherheitsbefragung 2015

Brunner, Alexander (2007): *Art. 163*, in: Niggli, Marcel Alexander / Wiprächtiger, Hans (Hrsg.): Strafrecht II, Art. 111–392 StGB. Basler Kommentar, 2. Aufl., Basel 2007, S. 785–797

Bundesamt für Lebensmittelsicherheit und Veterinärwesen (2019): OPSON VIII: Überprüfung von Kaffee-Kennzeichnungen. 06.2019.
https://www.newsd.admin.ch/newsd/message/attachments/57406.pdf [04.03.2020]

Bundesamt für Lebensmittelsicherheit und Veterinärwesen (2018a): OPSON VII: Wurde der Thunfisch «schöngefärbt»? 04.2018.
https://www.blv.admin.ch/dam/blv/de/dokumente/lebensmittel-und-ernaehrung/lebensmittelsicherheit/verantwortlichkeiten/bericht-eu-opson-thunfisch.pdf.download.pdf/Schlussbericht_OPSON_VII_DE.pdf [04.03.2020]

Bundesamt für Lebensmittelsicherheit und Veterinärwesen (2018b): Jahresbericht 2017 zu den Kontrollprogrammen an der Grenze. Überwachung von pflanzlichen Lebensmitteln und Gebrauchsgegenständen.
https://www.blv.admin.ch/dam/blv/de/dokumente/lebensmittel-und-ernaehrung/lebensmittelsicherheit/verantwortlichkeiten/bericht-grenzkontrollen-2017.pdf.download.pdf/Jahresbericht_Kontrollprogramme_an_der_Grenze_2017_zu_pflanzl._LM_und_GG_DE.pdf [04.03.2020]

Bundesamt für Lebensmittelsicherheit und Veterinärwesen (2016): Nationale Kampagne zum Nachweis von betrügerischen Praktiken bei der Vermarktung von Honigen und Fischen. https://www.blv.admin.ch/dam/blv/de/dokumente/lebensmittel-und-ernaehrung/lebensmittelsicherheit/verantwortlichkeiten/bericht-nat-kontrollprogramm-betrug-honig-fischen-2015.pdf.download.pdf/Rapport_pour_le_public,_campagne_authenticit%C3%A9_miels_et_poissons,_R%C3%A9sum%C3%A9_D_2.pdf [04.03.2020]

Bundesamt für Polizei fedpol (2020): Betrugsarten. https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/cybercrime/gefahren/betrugsarten. [04.03.2020]

Bundesamt für Polizei fedpol (2018): Gefahren im Internet. https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/cybercrime/gefahren.html. [04.03.2020]

Bundesamt für Polizei fedpol (2015): Jahresbericht der Nationalen Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIK 2014. https://www.fedpol.admin.ch/dam/data/fedpol/cybercrime/Berichte/2015-03-26/jb-2015-d.pdf [04.03.2020]

Bundesamt für Polizei fedpol (2014): Geldwäschereiurteile in der Schweiz. https://www.fedpol.admin.ch/dam/data/fedpol/publiservice/publikationen/berichte/geldwaeschereiurteile_okt2014-d.pdf [04.03.2020]

Bundesamt für Polizei fedpol (2011a): Jahresbericht 2010. Kriminalitätsbekämpfung Bund. https://www.fedpol.admin.ch/dam/data/fedpol/publiservice/publikationen/berichte/jabe/jabe-2010-d.pdf [04.03.2020]

Bundesamt für Polizei fedpol (2011b): Finanzagenten – Geldwäscherei als lukrative Nebenbeschäftigung (nicht veröffentlicht)

Bundesamt für Statistik (2019a): Strafurteilsstatistik. https://www.bfs.admin.ch/bfs/de/home/statistiken/kriminalitaet-strafrecht/strafjustiz.html [04.03.2020]

Bundesamt für Statistik (2019b): Polizeiliche Kriminalstatistik. https://www.bfs.admin.ch/bfs/de/home/statistiken/kriminalitaet-strafrecht/polizei.html [04.03.2020]

Bundesamt für Statistik (2019c): Zahl der Konkurseröffnungen steigt erneut an. Version vom 11.04.2019. https://www.bfs.admin.ch/bfsstatic/dam/assets/7966844/master [04.03.2020]

Bundesamt für Statistik (2019d): Polizeiliche Kriminalstatistik (PKS). Jahresbericht 2018 der polizeilich registrierten Straftaten. https://www.bfs.admin.ch/bfsstatic/dam/assets/7726191/master [04.03.2020]

Bundesamt für Statistik (2017): PKS – Polizeiliche Kriminalstatistik. Erfassungshilfe PKS V06.00. 01.01.2017. https://www.bfs.admin.ch/bfsstatic/dam/assets/2103675/master [04.03.2020]

Bundesanwaltschaft (2019): VW-Abgasmanipulationen: Online-Fragebogen für Geschädigte. Medienmitteilung vom 02.09.2019. https://www.bundesanwaltschaft.ch/mpc/de/home/medien/archiv-medienmitteilungen/news-seite.msg-id-76267.html [04.03.2020]

Bundesanwaltschaft (2014): Schweiz entschädigt Opfer im Fall Allen Stanford. Medienmitteilung vom 10.3.2014.
https://www.news.admin.ch/message/index.html?lang=de&msg-id=52261 [04.03.2020]

Bundesrat (2019): Strafprozessordnung soll praxistauglicher werden. 28.08.2019.
https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-76205.html.
[04.03.2020]

Bundesrat (2018): Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022.
https://www.isb.admin.ch/dam/isb/de/dokumente/ikt-vorgaben/strategien/ncs/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_DE.pdf.download.pdf/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_DE.pdf [04.03.2020]

Bundesrat (2013): Botschaft zur Umsetzung der 2012 revidierten Empfehlungen der Groupe d'action financière (GAFI) vom 13. Dezember 2013, BBl 2014 605.
https://www.admin.ch/opc/de/federal-gazette/2014/605.pdf [04.03.2020]

Bundesrat (2011): Botschaft zum Bundesgesetz über Lebensmittel und Gebrauchsgegenstände vom 25. Mai 2011, BBl 2011 5571.
https://www.admin.ch/opc/de/federal-gazette/2011/5571.pdf [04.03.2020]

Bundesrat (2009): Botschaft zur Änderung des Bundesgesetzes gegen den unlauteren Wettbewerb (UWG) vom 2. September 2009, BBl 2009 6151.
https://www.admin.ch/opc/de/federal-gazette/2009/6151.pdf [04.03.2020]

Bundesrat (1991): Botschaft über die Änderung des Schweizerischen Strafgesetzbuches und des Militärstrafgesetzes (Strafbare Handlungen gegen das Vermögen und Urkundenfälschung) sowie betreffend die Änderung des Bundesgesetzes über die wirtschaftliche Landesversorgung (Strafbestimmungen) vom 24. April 1991, BBl 1991 II 969.
https://www.amtsdruckschriften.bar.admin.ch/viewOrigDoc.do?id=10106593 [04.03.2020]

Chainalysis (2019): Crypto Crime Report. Decoding Hacks, Darknet Markets, and Scams.
https://blog.chainalysis.com/ 04.03.2020]

Der Bund (2016): Der Check als Auslaufmodell. 23.06.2016.
https://www.derbund.ch/wirtschaft/geld/der-check-als-auslaufmodell/story/wirtschaft/geld/der-check-als-auslaufmodell/story/wirtschaft/geld/der-check-als-auslaufmodell/story/17304703
[04.03.2020]

Egmont Group of Financial Intelligence Units (2019): *Business Email Compromise Fraud*, in: Egmont Group Bulletin.
https://www.egmontgroup.org/sites/default/files/filedepot/external/20190708_EGMONT%20GROUP%20BEC%20BULLETIN-final.pdf [04.03.2020]

EUROPOL (2019): 228 arrests and over 3800 money mules identified in global action against money laundering. Medienmitteilung vom 04.12.2019.
https://www.europol.europa.eu/newsroom/news/228-arrests-and-over-3800-money-mules-identified-in-global-action-against-money-laundering [04.03.2020]

EUROPOL (2016): EUROPOL strengthens efforts to tackle social engineering. Medienmitteilung vom 28.01.2016.
https://www.europol.europa.eu/latest_news/europol-strengthens-efforts-tackle-social-engineering [04.03.2020]

Europäische Kommission (2018): Knowledge Centre for Food Fraud and Quality. Infographic.
https://ec.europa.eu/knowledge4policy/sites/know4pol/files/a0infographic_kc_food_fraud_final_0.pdf [04.03.2020]

Fiolka, Gerhard (2019): *Art. 147*, in: Niggli, Marcel Alexander / Wiprächtiger, Hans (Hrsg.): Strafrecht II, Art. 111–392 StGB. Basler Kommentar, 4. Aufl., Basel 2019, S. 3160-3178

Galli, Peter / Moser, André / Lang, Elisabeth / Steiner Marc (2013): Praxis des öffentlichen Beschaffungsrechts. Eine systematische Darstellung der Rechtsprechung des Bundes und der Kantone. 3. Auflage. Zürich 2013

Groupe d'action financière GAFI (2013): National Money Laundering and Terrorist Financing Risk Assessment. FATF Guidance, February 2013.
www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf [04.03.2020]

Groupe d'action financière GAFI (2012): International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations. Aktualisiert im Juni 2019.
https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf [04.03.2020]

Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung KGGT (2018a): Bericht über die Bargeldverwendung und deren Missbrauchsrisiken für die Geldwäscherei und Terrorismusfinanzierung in der Schweiz. Oktober 2018
https://www.newsd.admin.ch/newsd/message/attachments/55177.pdf [04.03.2020]

Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung KGGT (2018b): Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding. Oktober 2018
https://www.newsd.admin.ch/newsd/message/attachments/56167.pdf [04.03.2020]

Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung KGGT (2017): Geldwäschereirisiken bei juristischen Personen. November 2017.
https://www.fedpol.admin.ch/dam/data/fedpol/kriminalitaet/geldwaescherei/nra-berichte/nra-bericht-nov-2017-d.pdf [04.03.2020]

Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung KGGT (2015a): Bericht über die nationale Beurteilung der Geldwäscherei- und Terrorismusfinanzierungsrisiken in der Schweiz. Juni 2015.
https://www.fedpol.admin.ch/dam/data/fedpol/kriminalitaet/geldwaescherei/nra-berichte/nra-bericht-juni-2015-d.pdf [04.03.2020]

Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung KGGT (2015b): Medienmitteilung zum Bericht über die nationale Beurteilung der Geldwäscherei- und Terrorismusfinanzierungsrisiken in der Schweiz. Juni 2015.
https://www.news.admin.ch/message/index.html?lang=de&msg-id=57750 [04.03.2020]

Levi, Michael (2008): *Organized fraud and organizing frauds: Unpacking research on networks and organization*, in: Criminology and Criminal Justice, Vol 8(49), S. 389-419.
https://www.researchgate.net/profile/Michael_Levi4/publication/249786379_Organized_fraud_and_organizing_fraudsUnpacking_research_on_networks_and_organization/links/0c960532755df02414000000/Organized-fraud-and-organizing-fraudsUnpacking-research-on-networks-and-organization.pdf [04.03.2020]

Maeder, Stefan/ Niggli, Marcel Alexander (2019): *Art. 146*, in: Niggli, Marcel Alexander / Wiprächtiger, Hans (Hrsg.): Strafrecht II, Art. 111–392 StGB. Basler Kommentar, 2. Aufl., Basel 2019, S. 3084-3159

NTV (2012): Handel mit Falsch-Käse entlarvt. 17.06.2012. https://www.n-tv.de/panorama/Handel-mit-Falsch-Kaese-entlarvt-article6750746.html [04.03.2020]

PricewaterhouseCoopers (2018): Gesunken, aber nicht geschlagen: Schweizer Wirtschaftskriminelle werden digital und suchen sich neue Tätigkeitsfelder. Globale Umfrage zur Wirtschaftskriminalität 2018 – Schweizer Erkenntnisse. https://www.pwc.ch/de/publications/2018/globale-umfrage-zur-wirtschaftskriminalitaet-2018.pdf [04.03.2020]

RTS (2013): Du cheval à la place de boeuf dans des tartares servis en Suisse. https://www.rts.ch/info/suisse/5329304-du-cheval-a-la-place-de-boeuf-dans-des-tartares-servis-en-suisse-.html [04.03.2020]

Sakic, Senad (2015): Gewerbsmässige Firmenbestattung. Masterarbeit am Competence Center Forensik und Wirtschaftskriminalität. Hochschule Luzern. Luzern 2015

Schweizerische Versicherungsverband SVV (2017): Versicherungsbetrug: Zahlen und Fakten. Zusammenfassung der Ergebnisse der GfK Studie zum Versicherungsmissbrauch. 31.08.2017. https://www.svv.ch/sites/default/files/2017-11/SVV%20Zusammenfassung%20der%20Ergebnisse%20der%20GfK%20Studie%20zum%20Versicherungsmissbrauch%202017.pdf [04.03.2020]

SRF (2016): Konkursreiterei: Mehrere Hundert Millionen Schaden im Jahr. 13.04.2016. https://www.srf.ch/news/schweiz/konkursreiterei-mehrere-hundert-millionen-schaden-im-jahr [04.03.2020]

Trechsel, Stefan / Crameri, Dean (2012): *Art. 146 Betrug*, in: Trechsel, Stefan / Pieth, Mark (Hrsg.): Schweizerisches Strafgesetzbuch Praxiskommentar, 2. Aufl., Zürich 2012, S. 736–766

Weissenberger, Philippe (2019): *Art. 172ter*, in: Niggli, Marcel Alexander / Wiprächtiger, Hans (Hrsg.): Strafrecht II, Art. 111–392 StGB. Basler Kommentar, 4. Aufl., Basel 2019, S. 3550-3563

Urteile des Bundesgerichts:

BGE 116 IV 343. http://relevancy.bger.ch/php/clir/http/index.php?highlight_docid=atf%3A%2F%2F116-IV-343%3Ade&lang=de&type=show_document [04.03.2020]

BGE 126 IV 165. http://relevancy.bger.ch/php/clir/http/index.php?lang=de&zoom=&type=show_document&highlight_docid=atf%3A%2F%2F126-IV-165%3Ade [04.03.2020]

BGE 129 IV 315. http://relevancy.bger.ch/php/clir/http/index.php?lang=de&zoom=&type=show_document&highlight_docid=atf%3A%2F%2F129-IV-315%3Ade [04.03.2020]

BGE 134 IV 210. http://relevancy.bger.ch/php/clir/http/index.php?lang=de&zoom=&type=show_document&highlight_docid=atf%3A%2F%2F134-IV-210%3Ade [04.03.2020]

BGE 124 IV 274. http://relevancy.bger.ch/php/clir/http/index.php?highlight_docid=atf%3A%2F%2F124-IV-274%3Ade&lang=de&type=show_document [04.03.2020]

Urteil (des Bundesgerichts) 1A.189/2001 vom 22.02.2002. www.polyreg.ch/bgeunpub/Jahr_2001/Entscheide_1A_2001/1A.189__2001.html [04.03.2020]

Urteil (des Bundesgerichts) 6P.172/2000 und 6S.776/2000 vom 14.5.2001. www.polyreg.ch/bgeunpub/Jahr_2000/Entscheide_6P_2000/6P.172__2000.html [04.03.2020]

Urteil des Bundesstrafgerichts:

Urteil (des Bundesstrafgerichts) SK.2010.9 vom 24.11.2010. https://bstger.weblaw.ch/cache/pub/cache.faces?file=20101124_SK_2010_9.htm&ul=fr [04.03.2020]