

Daniel Fischer, Zürich

Crime Due Diligence – eine Verdachtsschöpfungsstrategie¹

Inhaltsübersicht

- I. Ausgangslage
- II. Der Begriff der Crime Due Diligence
- III. Abgrenzung zu anderen Methoden
- IV. Materielle und formelle Crime Due Diligence
- V. Analysen
 - A) Personenanalyse
 - B) Dokumentenanalyse
 - C) Strukturanalyse
 - D) Übersichtsschema
- VI. Anwendbarkeit der Analysen
- VII. Schlussbemerkung

I. **Ausgangslage**

In den letzten Jahren haben sich die Delikte gegen die Wirtschaftsgüter verändert². Diese Entwicklung ist im Wesentlichen auf zwei Faktoren zurückzuführen:

- Zum einen machte die Informationsdigitalisierung die Wirtschaft schneller, anonym und grenzüberschreitender. Dies erlaubt es, die Delikte effizienter und in einer bis anhin ungeahnten Grössenordnung und Geschwindigkeit zu begehen³.

1 Meinem juristischen Mitarbeiter Rechtsanwalt lic. iur. Pascal Honold, Zürich, danke ich für die Unterstützung beim Verfassen dieses Beitrags und Kai-D. Bussmann, Professor an der Martin-Luther-Universität Halle-Wittenberg, Christian Weber, Staatsanwalt des Kantons Zürich, Thomas Armbruster, Bezirksanwalt des Kantons Zürich, Felix Weingartner, Fahnder der Kantonspolizei Zürich, Rechtsanwalt Lucius Blattner, CFE, sowie Rechtsanwalt Thomas Schwyzer, Zürich, für ihre wertvollen Anregungen.

2 G. Dannecker, in: Handbuch des Wirtschafts- und Steuerstrafrechts, hrsg. von H.-B. Wabnitz/T. Janovsky, München 2000, 6.

3 So auch R. Müller/H.-B. Wabnitz/T. Janovsky, Wirtschaftskriminalität. Eine Darstellung der typischen Erscheinungsformen mit praktischen Hinweisen zur Bekämpfung, 4. Aufl., München 1997, 37: «Die technische Entwicklung und der weltweite schrankenlose Einsatz der Computer- und Informationstechnologie hat die nationalen Gesetzgeber [...], insbesondere die Ermittlungsbehörden überrollt.»

- Zum anderen entstanden vielfältige, zuweilen auch sehr komplizierte Investitionsformen auf dem Finanzmarkt⁴. Die Anleger waren es gewohnt, dass sie die immer komplexer werdenden Anlagemechanismen nicht mehr wirklich verstanden, und wurden so anfälliger für schwer durchschaubare, kriminelle Finanztransaktionen.

Diese Ausgangslage wurde von raffinierten Schwindlern ausgenutzt, welche durch ausgeklügelte Vorgehensweisen und überlegene Kommunikation⁵ die Opfer übertölpelten.

Die oben erwähnten Veränderungen sind so gravierend, dass man gar von einer neuen Dimension von Wirtschaftsdelikten sprechen kann. In der Lehre werden sie einerseits immer noch mit Wirtschaftskriminalität⁶ oder «white collar crime»⁷ bezeichnet, andererseits sind aber auch neue Termini wie unter anderem «Finanzbetrug»⁸ oder «New Econ Crime»⁹ auszumachen¹⁰. Diesen Erscheinungsformen

4 Vgl. Report der Bank for International Settlements, Februar 2003. Der Markt für ausserhalb der Börse gehandelte Derivative wuchs im ersten Halbjahr 2002 um 15% auf eine Rekordsumme von US\$ 128 Billionen. Dieser Wert der gehandelten Derivative, welcher an den zu Grunde liegenden Assets gemessen wird, ist viermal höher als das Volumen der Bruttoinlandprodukte der gesamten Weltwirtschaft.

5 Siehe dazu ausführlich unter V. C 1.

6 K. Boers, Wirtschaftskriminologie. Vom Versuch, mit einem blinden Fleck umzugehen, Monatschrift für Kriminologie und Strafrechtsreform, Heft 5 (2001) 335, wonach die kriminologische Forschung zur Wirtschaftskriminalität seit jeher mit begrifflichen, methodischen und theoretischen Schwierigkeiten konfrontiert ist; ähnlich G. Nay, in: Basler Kommentar, Strafgesetzbuch II, Art. 111–401 StGB, Basel 2003, Art. 340^{bis} N 5, hrsg. von M. Niggli/H. Wiprächtiger; Kritik am Begriff unter G. Kaiser, Kriminologie, Ein Lehrbuch, 3. Aufl., Heidelberg 1996, 855 ff.

7 E. H. Sutherland, White Collar Crime. The uncut version. With an introduction by Gilbert Geis and Colin Goff, New Haven/London 1983, 7.: «White Collar Crime is a crime committed by a person of respectability and high social status on the course of his occupation»; vgl. auch Dannecker (Fn. 2), 8: «White collar crime» bezeichnet im engeren Sinn Straftaten, die von ehrbaren Personen mit hohem sozialen Ansehen im Rahmen ihrer beruflichen Tätigkeit verübt werden. Diese Eigenschaften treffen in der Regel auf die hier beschriebenen Täter nicht zu; ebenso Boers (Fn. 6), 338; vgl. auch die ausführliche Kritik in K.-L. Kunz, Zum Verständnis der Kriminalität des Weissen Kragens. Auf der Spur eines in Verruf geratenen Konzepts, in: Wirtschaft und Strafrecht, Festschrift für Niklaus Schmid, hrsg. von J.-B. Ackermann/A. Donatsch/J. Rehberg, Zürich 2001, 94 ff; ebenfalls sehr kritisch D. Nelken, White-Collar Crime, in: The Oxford Handbook of Criminology, hrsg. von M. Maguire/R. Morgan/R. Reiner, 3. Aufl., Oxford 2002, 844 ff.

8 M. Glinig, Der internationale Finanzbetrug, 3. Aufl., Wien 2000, 7. Darunter versteht der Autor den Betrug gegen Banken und den Betrug im Zusammenhang mit Finanzdienstleistungen sowie den Betrug mit Finanzpapieren wie Scheck, Wechsel und Wertpapieren.

9 D. Fischer, in: Finanz- und Rechnungswesen, Jahrbuch 2003, hrsg. von H. Siegwart, Zürich 2003, 208, wonach unter New Econ-Crime die Verletzung von strafrechtlich geschützten Wirtschaftsgütern verstanden wird, hauptsächlich durch Mittel der Datenkommunikation, wobei mit geringem Aufwand ein verhältnismässig grosser Schaden verursacht wird; D. Fischer, in: Meilensteine im Management, Band X, Management & Law, hrsg. von H. Siegwart/J. Mahari, Basel 2003, 361 ff.

10 M. Killias, Von «White Collar Crime» zur organisierten Kriminalität: Zeitgenössische Inkarnation des Bösen, in: Festschrift für Niklaus Schmid, Wirtschaft und Strafrecht, hrsg. von J.-B. Ackermann/A. Donatsch/J. Rehberg, Zürich 2001, 71 ff.; ebenso Kunz (Fn. 7), 87 ff.

müssen darum neue Erkennungsmethoden entgegengesetzt werden, welche die oben genannte Informationsdigitalisierung und Anonymität der Kapitalwirtschaft berücksichtigen.

Die Voraussetzung des Erkennens beziehungsweise des Aufdeckens eines Verbrechens ist der Verdacht. Der intuitiven Verdachtsschöpfung¹¹ stehen wissenschaftliche oder empirische Verdachtsschöpfungsstrategien gegenüber. Infolge der erhöhten Komplexität der Delikte ist die intuitive Verdachtsschöpfung erschwert oder gar völlig ausgeschlossen. Das Opfer erkennt häufig zu lange nicht, dass es Ziel eines kriminellen Angriffs ist.

Dieser Aufsatz handelt insbesondere von Erkennungsstrategien gegen unterschiedlichste Täuschungsszenarien, die darauf abzielen, die Täter auf Kosten der Opfer zu bereichern.

II. Der Begriff der *Crime Due Diligence*

In Europa versteht man unter einer *Due Diligence*¹² eine umfassende Abklärung der finanziellen und rechtlichen Verhältnisse, welche Firmen vor einer Unternehmensübernahme durchführen. In den USA geht dieser Begriff weiter, er wird ganz allgemein bei Abklärungen wirtschaftlicher Vorgänge verwendet; so wird zum Beispiel auch bei einer Produkteinführung eine *Due Diligence* betreffend Umweltverträglichkeit und Konsumentenfreundlichkeit in Auftrag gegeben.

Im heutigen Wirtschaftsumfeld bedarf es bei einer Finanzoperation auch der Abklärung des möglichen Konnexes zu kriminellen Machenschaften. Diese Untersuchung wird in der Folge *Crime Due Diligence* genannt. Sie besteht aus der Personen-, Dokumenten- und Strukturanalyse. In diesen segmentierten Bereichen sollen Risikofelder erkennbar gemacht werden. Im Rahmen der Analysen erfolgt ein Datenabgleich. Dieser beruht einerseits auf Erkenntnissen der Fahndungsbehörden und andererseits auf der konkret vorgetragenen und/oder dokumentierten «Tatgeschichte».

Die Analysen werden mit Hilfe von so genannten Modulen vorgenommen. Module sind austauschbare Elemente eines ganzen Systems¹³. Grundsätzlich treten selten alle Module gemeinsam in Erscheinung. Die Tätererkennung beruht auf der Bewertung verschiedener, in einem bestimmten Fall erkennbarer Module.

Die Zuordnung der Module unter die jeweiligen Analysen ist nicht immer offensichtlich. Die Module werden nach Erfahrungswerten gewichtet und entsprechend

11 U. Störzer, in: *Kriminalistik, Handbuch für Praxis und Wirtschaft*, Band 1, hrsg. von E. Kube/U. Störzer/K. Timm, Stuttgart/München/Hannover/Berlin/Weimar 1992, 430.

12 E. Ellen, *Special Report Due Diligence*, ICC – International Maritime Bureau, Paris 1994, 1 ff.

13 F. A. Brockhaus, «Der Brockhaus» Computer und Informationstechnologie, Mannheim 2002.

ihres Kerngehaltes eingefügt. Das «Brand»-Modul¹⁴ beispielsweise hat einen engen Bezug sowohl zu den involvierten Personen als auch zur Verbrechenstruktur. U.E. ist das «Brand»-Modul jedoch schwergewichtig Bestandteil der Personenanalyse.

III. Abgrenzung zu anderen Methoden

Über die meisten Delikte liegt in der Regel eine Fülle von Informationen bzw. Daten vor. Werden nun diese Daten gesammelt, geordnet und verglichen, besteht die Möglichkeit, aus ihnen bestimmte Merkmale abzuleiten, welche einer bestimmten Deliktsart eigen sind. Diese Merkmale, welche aus den Datenabgleichen gewonnen werden, können verbrechensverhütend und -aufklärend verwendet werden. Die Crime Due Diligence basiert grundlegend auf der Idee des Datenabgleichs. Daher sollen nachfolgend die Entstehung des Datenabgleichs und der Methoden, welche auf diesem beruhen, beleuchtet bzw. verglichen werden.

Erstmals auf das Prinzip des Datenvergleichs machte am Anfang des letzten Jahrhunderts Weingart¹⁵ mit seinen «Methoden zur Ermittlung und Überführung des Täters» aufmerksam. Jäger¹⁶ differenzierte die Verbrechensmerkmale mit der Kriminologie der Einzeldelikte in Form von Bearbeitungsschemen sowie mit ihrer Entstehung, geordnet nach Unterpunkten von Tatzeit bis Tatort. Die Polizei entwickelte darauf basierend die so genannten Jägerschen Schemen. Die Praxis machte sie später als Verdachtsschöpfungskalender¹⁷ anwendbar. Diese Checklisten sind sehr hilfreich; auf dem gleichen Prinzip beruhen die Verdachtsraster¹⁸. Die klassische Polizeiarbeit ist der Vergleich aufgedeckter Straftaten und deren Muster mit unaufgelösten Fällen und damit die Zuordnungsversuche solcher Taten anhand der gefundenen Parallelen (kriminalpolizeilicher Meldedienst mit Modus operandi System¹⁹).

Eine weitere bedeutende Methode, welche auf dem Datenabgleich beruht, ist das Profiling²⁰. Die Grundlagen des kriminalistischen Profilings legte 1880 der

14 Ausführlich unter V. A 2. «Brand»-Modul.

15 A. Weingart, *Kriminaltaktik. Ein Handbuch für das Untersuchen von Verbrechen*, Leipzig 1904, 94 ff.

16 J. Jäger, *Kriminologie und Kriminalitätskontrolle. Grundriss einer anwendungsorientierten Kriminologie*, Lübeck 1981, 46 ff.

17 Vgl. dazu M. Tecl, *Ist Kriminologie auch für die Schutzpolizei wichtig? Der «Verdachtsschöpfungskalender» als wichtige Hilfe*, Deutsches Polizeiblatt 7 (1989) Heft 2, 3.

18 Störzer (Fn. 11), 448.

19 Vgl. dazu W. Burghard, *Einführung in die Kriminalistik, Lehr- und Studienbriefe Kriminalistik I* (1997) 18.

20 Siehe dazu S. Harrison, *The Diary of Jack the Ripper: The Chilling Confessions of James Maybrick*, London 1993, 1 ff.; B. E. Turvey, *Criminal Profiling, An Introduction to Behavioural Evidence Analysis*, London 1999, 1 ff.; C. B. Meyer, *Das Täterprofil aus interdisziplinärer Sicht, unter besonderer Berücksichtigung des Strafprozessrechts*, in: *Information und Recht*, hrsg. von M. Cottier/D. Rüetschi/K. W. Sahlfeld, Basel 2002, 135 ff.

Psychologe Dr. Thomas Bond. Er beschrieb verschiedene Methoden zur Tätercharakterisierung und Täterermittlung aufgrund konkreter Tatinformationen und der Berücksichtigung anderer Delikterkenntnisse sowie statistischer Erhebungen. Diese Methoden nannte er Profiling²¹. Im Gegensatz zur Crime Due Diligence wird beim Profiling hauptsächlich bezweckt, den Täter nach begangener Tat (und evtl. vor erneuter Tat) «hochzurechnen», d.h., anhand von Charakteristika neue Taten vorzusehen, wogegen die Crime Due Diligence das potenzielle Opfer überhaupt erst auf die Möglichkeit einer kriminellen Tat aufmerksam machen und dieses dann davor bewahren will.

Die Ermittlungsbehörden fanden in den 80er-Jahren eine ähnliche wie die eingangs beschriebene, heutige Ausgangslage vor. Sie wurden mit einer völlig neuen Form von Gewaltverbrechen (und nicht wie heute Wirtschaftsverbrechen), nämlich dem Terrorismus²², konfrontiert.

Die Polizei setzte damals diesen Erscheinungsformen der Kriminalität neue Methoden der Verbrechensbekämpfung entgegen: der vermehrte Einsatz von V-Leuten²³, polizeilicher Abhörung²⁴ und insbesondere der Rasterfahndung²⁵ sollte Hilfe bringen. Bei der Rasterfahndung zielen die polizeilichen Eingriffe nicht mehr gegen einzelne Tatverdächtige. Gegenstand der polizeilichen Aktivität werden alle Personen, die Träger gleicher persönlicher Merkmale sind. Rasterfahndung zielt darauf ab, mit Hilfe elektronischer «Merkmalsraster» aus einer beliebig grossen Personenzahl eine kleinere herauszufiltern, bei welcher die Wahrscheinlichkeit des Tatverdachts grösser ist. Es werden so lange Verdächtige herausgesiebt, bis eine kleine Zahl von möglichen Tätern verbleibt, die mit herkömmlichen Methoden genauer überprüft werden kann. Davon ausgehend, dass beispielsweise Terroristen ihre Stromrechnung nicht selbst oder nur bar bezahlen, wurden die Kundendaten der Hamburger Elektrizitätswerke nach solchen Strombezügern überprüft²⁶; rasterverdächtig sind auch Mietbarzahlungen, Telefone ohne Gebührenanfall, Mietverhältnisse in der Nähe von US-Militärkasernen usw. Dieses negative Ausleseverfahren führte zu einer Umkehrung des normalen Ermittlungsganges und wurde als Zweckentfremdung²⁷ der Daten kritisiert.

21 A. von Lüpke, Täterprofile. Crime Profiling – eine «neue» Form der Verdachtsstrategie, Kriminalistik 53 (1999) 814 ff. Er definiert das Täterprofil wie folgt: Die «Zusammenstellung von Merkmalen zu einem mehr oder weniger genauen Bild eines noch unbekanntes Täters, der mit Hilfe dieser Bilder ermittelt werden soll».

22 Gemeint ist hierbei u.a. der politische Terrorismus der Roten Armee Fraktion (RAF) in Deutschland.

23 K. Rogall, Moderne Fahndungsmethoden im Lichte gewandelten Grundrechtsverständnisses, GA 1985, 2.

24 Ebda.

25 Siehe dazu einlässlich J. Simon/J. Taeger, Rasterfahndung: Entwicklung, Inhalt und Grenzen einer kriminalpolizeilichen Fahndungsmethode, Baden Baden 1981, 1 ff. Siehe dazu auch J. Simon/J. Taeger, Grenzen kriminalpolizeilicher Rasterfahndung, JZ 1982, 141.

26 Simon/Taeger (Fn. 25), 23.

27 Rogall (Fn. 23), 5.

Nachdem auch die Rasterfahndung auf die Tätererkennung bzw. -ermittlung fokussiert ist, steht sie im Gegensatz zur Crime Due Diligence, welche sich darauf konzentriert, die Frage zu beantworten, ob überhaupt eine strafrechtlich relevante Tat vorliegt. Die Crime Due Diligence ist somit eine Tätererkennungsmethode. Aus der Sicht des Opfers soll die Vollendung der Tat verhindert werden. Die Gemeinsamkeit der «Jägerschen» Schemen, der Verdachtskalender, des Profiling und der Rasterfahndung mit der Crime Due Diligence besteht letztlich darin, dass diese Methoden spezifisch definierte Merkmale in Bezug zu Daten setzen.

IV. **Materielle und formelle Crime Due Diligence**

Grundsätzlich kann bei der Crime Due Diligence zwischen materiellen und formellen Komponenten unterschieden werden. Die materiellen Merkmale haben unmögliche oder erwiesenermassen unwahre Sachverhalte zum Inhalt, wohingegen sich formelle Anhaltspunkte an äusserlichen Kennzeichen orientieren. In der Semiotik entspricht das materielle Element dem Signifikat, das formelle Element dem Signifikant.

Nachstehend zwei Beispiele für materielle Erkenntnisse:

- *Am 14.4.2000 wurde ein Gold-Zertifikat der Firma Ambel Overseas Ltd. in Zürich im Betrage von nicht weniger als US\$ 14 Milliarden in Goldreserven gehandelt. Tatsache ist nun aber, dass der grösste Goldfund, der in den letzten zehn Jahren weltweit gemacht wurde, einen Wert von US\$ 330 Millionen hatte. (Goldminenfall)*
- *Im April 2001 kam in Zürich ein Certificate of Deposit auf den Markt, welches die Chase Manhattan Bank als federführende Referenzbank ausgab. Der Wert des Certificates belief sich angeblich auf US\$ 950 Millionen. Die Untersuchung ergab, dass die Chase Manhattan Bank zum fraglichen Zeitpunkt gar nicht mehr existierte und deren Rechtsnachfolgerin, die JP Morgan, ein solches Certificate nie übernommen hat. (Chase-Manhattan-Fall)*

Ergibt also die Personenanalyse, dass eine Person erwiesenermassen nicht existiert, ist dies eine materielle Erkenntnis, die den vorgetragenen Sachverhalt vorweg als deliktisch entlarvt. Unter formellen Anhaltspunkten hingegen sind beispielsweise Briefkastenfirmen²⁸ auf bekannten Offshore-Finanzplätzen oder Transaktionen mit ungewöhnlich hohen Beträgen zu verstehen. Ein formeller Anhaltspunkt alleine ist jedoch kein überzeugender Beweis, dass betrügerische Operationen vorliegen. Erst die Vielzahl bzw. die Kombination einzelner Merkmale macht die Wahrscheinlichkeit grösser. So ist schwer einzusehen, weshalb Transak-

28 Müller/Wabnitz/Janovsky (Fn. 3), 259.

tionen von Riesenbeträgen über Offshore-Gesellschaften abgewickelt werden, welche sich keine anständigen Bürostrukturen leisten können und ein Firmenkapital von wenigen Franken haben.

Es versteht sich von selbst, dass Module sowohl materieller als auch formeller Natur sein können. Die Crime Due Diligence betrachtet eine Transaktion in der materiellen und zeitlichen Gesamterscheinung. Die Unzulänglichkeiten des Finanzgeschäfts werden in den verschiedenen Phasen erkenntlich.

V. Analysen

A) Personenanalyse

Die Personenanalyse zielt in ihrem Anwendungsbereich auf die handelnde Täterpersönlichkeit²⁹ bzw. die darin involvierten Handlungsfiguren. Sie prüft zum einen die Namen der Täter, sei es eine natürliche oder auch juristische Person (Verstrickungsmodul), deren Wohnort (Offshore-Modul), die Staatszugehörigkeit (Nationalitätenmodul) und orientiert sich damit an konkreten Zielvorgaben. Sie beschäftigt sich aber zum anderen abstrakt mit jenen Namen, welche die Täter prioritär gebrauchen (Brand-Modul), und mit generellen Verhaltensmuster solcher Täter (Hochstaplermodul).

Bei betrügerischen Vorgängen ist die kriminelle Handlungsfigur entscheidend. Die Täter wissen ob der Gefährlichkeit der Aufdeckung ihrer Identität. Sie verwenden deshalb üblicherweise zwei Schutzszenarien. Einerseits wechseln sie bewusst die Schreibweise ihres Vor- und Nachnamens, z.B. James Miller wird zu John Mullen, dabei die Erkenntnis ausnützend, dass Datenbanken nur Resultate liefern, wenn die korrekte Schreibweise eingegeben wird. Andererseits bleiben die Täter im Hintergrund und schieben möglicherweise nichts ahnende Personen vor. So ist der «Frontman»³⁰ als jene Person bekannt, die offiziell als Verantwortliche eines kriminellen Unternehmens figuriert. «Goofer»³¹ und «Runner»³² verüben hingegen untergeordnete Tätigkeiten im kriminellen Netzwerk. Ein wichtiger Bestandteil des Netzwerks ist der so genannte «Finder»³³, der einzig die Aufgabe hat, Opfer ausfindig zu machen und sie zu überzeugen.

29 Unterschied Profiling zur Personenanalyse: Beim Profiling geht es darum, das Verhalten des Täters zu rekonstruieren, bei der Personenanalyse geht es um die Täterpersönlichkeit als solche. Profiling wird im Übrigen nicht in der Bekämpfung von Wirtschaftsdelikten genutzt; siehe auch Meyer (Fn. 20), 151.

30 Definition bei Glinig (Fn. 8), 154: gegen aussen als Verantwortlicher auftretend.

31 Definition bei Glinig (Fn. 8), 154: Laufbursche zur Besorgung untergeordneter Tätigkeit.

32 Definition bei Glinig (Fn. 8), 154: Laufbursche zur Besorgung untergeordneter Tätigkeit.

33 Definition bei Glinig (Fn. 8), 154: Krimineller, der die Opfer ausfindig macht und gegen Provision weitervermittelt.

1. Verstrickungsmodul

Als primärer Prüfungsschritt definiert sich das Verstrickungsmodul. Darunter wird das Ausfindigmachen von Personen resp. Unternehmen anhand von recherchierten Informationen verstanden, sei es über das Zielobjekt selber oder über Figuren aus dessen Umfeld, die in anderen unlauteren Transaktion aufgefallen sind. Im Goldminenfall³⁴ war beispielsweise der Haupttäter vor Jahren in einem betrügerischen Zigarettenarbitragegeschäft in Erscheinung getreten.

Erschwert ist das Herausarbeiten des Verstrickungszusammenhangs bei der Untersuchung einer Unternehmensbezeichnung, da juristische Personen häufig bloss vorgeschoben sind, um Hintermänner zu verbergen³⁵. Dies fällt besonders leicht, weil Firmen schnell gegründet oder durch die Übernahme von Firmennäntel einfach benutzt werden können. Die Identitätssuche kann auch mit Firmennamensänderungen, die ebenfalls mit wenig Aufwand verbunden sind, erschwert werden.

Der Verstrickungszusammenhang wird mit Hilfe von Datenbanken, mit Vorteil aus verschiedenen breitgefächerten, internationalen Quellen, generiert. Die in Zentraleuropa vorherrschende Sensibilität für datenschützerische Anliegen³⁶ verhindert häufig tiefgehende Personenanalysen, wohingegen dies im anglo-amerikanischen Raum *courant normal* darstellt. Dort werden sogar Verdächtige oder Angeklagte in den Zeitungen namentlich erwähnt. In den USA besteht darüber hinaus ein (beschränkter) öffentlicher Zugang zu Gerichts dossiers, zu Polizeirapporten und Führerscheinpapieren.

Der gesamte Inhalt tausender Zeitungen und Magazine wird weltweit in Mediendatenbanken angeboten, die man über so genannte Hosts wie Lexis-Nexis, Reuter (Newline), Dialog und Datastar usw. abrufen kann³⁷. Das grösste zugängliche Pressearchiv ist die «Dow Jones Interactive Library»³⁸. Empfehlenswert ist auch die «Electric Library»³⁹ und das Pressearchiv der «Financial Times»⁴⁰. Im deutschsprachigen Raum sei anstelle von vielen auf die Firma «Genios»⁴¹ verwiesen. Aber auch themenspezifische Chat-Rooms sind eine erspriessliche Quelle für Daten⁴². Gleichzeitig ist jedoch auch auf die besondere Gefahr von Falschinformationen hinzuwei-

34 Siehe Beispiel unter IV.

35 In Analogie dazu: die französische Bezeichnung für Aktiengesellschaft «société anonyme»; siehe Lösungsvorschlag betreffend Strafbarkeit juristischer Peronen in *R. Roth, Responsabilité pénale de l'entreprise: modèles de réflexion, Revue pénale suisse, 115 (1997) 345–381.*

36 Bundesgesetz vom 9. Juni 1992 über den Datenschutz [DSG], SR 235.1.

37 Ähnlich *Glinig* (Fn. 8), 133.

38 Siehe <http://djinteractive.com>.

39 <http://www.elibrary.com>.

40 <http://www.globalarchive.ft.com>.

41 <http://www.genios.de>.

42 Als ein Beispiel unter vielen: «<http://www.ragingbull.altavista.com>»

sen, die von den Betrügern absichtlich zur Verwirrung und Irreführung im Chat-Room gezielt gestreut werden. Bekanntes Szenario hierfür ist, wenn ein Opferanwalt von den Kriminellen warnend als Vertreter der Täter bezeichnet wird.

Die Verstrickungsmethode versucht somit, die gesammelten Einzelinformationen zueinander auf einer Datenbank in Bezug zu setzen, sodass daraus ein Informationsgesamtbild entsteht.

2. «Brand»-Modul

Das Vertrauen der Opfer wird erschlichen, wenn der «Brand»⁴³ einer weltbekannten Unternehmung nachgeahmt wird, sodass auf den ersten Blick der Unterschied zum Original nicht ersichtlich ist. Auch pompöse Briefköpfe, welche leicht mit einem Laserdrucker nachzumachen sind, sollten per se zur Vorsicht mahnen. Häufig kopierte Firmen sind Lloyd's alias Lloyds, Rotschild alias Rothschild, Capital Suisse⁴⁴ alias Credit Suisse, United Bank of Switzerland alias UBS AG oder als aktuelles Beispiel der als betrügerisch geltende Investmentfond OPEC Fund in Mexiko, der in keiner Beziehung zur OPEC steht⁴⁵. In letzter Zeit werden vermehrt auch religiöse Institutionen in betrügerischer Absicht nachgeahmt⁴⁶.

3. Offshore-Modul⁴⁷

Gesellschaften mit Adressen auf Offshore-Plätzen⁴⁸ und geringem Eigenkapital sind ein klares formelles Kennzeichen. Es ist unrealistisch, dass Millionenoperationen teilweise über undurchsichtige Einheiten ohne adäquate Kapitaldecke vollzogen werden. Finanzgesellschaften, welche die Fähigkeiten besitzen, derartige Finanztransaktionen durchzuführen, verfügen über eine entsprechende professionelle Infrastruktur und bedienen sich offensichtlich nicht eines Business-Centers für ihre Dienstleistungen.

43 Unter «brand» versteht der Verfasser eine weltweit bekannte Marke, die einen hohen Reputationswert besitzt. Gemeint ist das Zusammenspiel zwischen Label, Produktauftritt, Namen und Werbung, welche den Marktauftritt prägen.

44 <http://www.capitalsuisse.com>.

45 Organization of the Petroleum Exporting Countries (OPEC). Siehe Warnhinweis auf <http://www.opecfund.org>.

46 Vgl. V. C) 2. b) Wohltätigkeitsmodul.

47 Müller/Wabnitz/Janovsky (Fn. 3), 260, «Weisse-Kragen-Täter» haben erkannt, dass durch Einschaltung von Briefkastenfirmen nicht nur Steuerdelikte, sondern alle übrigen Wirtschaftsstraf-taten ermöglicht und erleichtert werden.

48 Wie Cook-Inseln, Nauru, Liberia, Bermudas, Vanuatu.

4. *Nationalitätenvermutungsmodul*

Unter diesem Modul wird die Notwendigkeit erhöhter Abklärungen über die Zugehörigkeit involvierter Akteure zu spezifischen Staaten verstanden. Die Nationalitätenvermutung spielt bei Anbietern von Finanzgeschäften aus sensitiven Ländern oder Regionen eine bedeutende Rolle⁴⁹. Vor allem institutionelle Anleger führen schwarze Listen mit Staaten, welchen die Nationalitätenvermutung anhaftet. Das hat zur Folge, dass Anbietern aus solchen Staaten in erhöhtem Masse investigativ begegnet werden muss. Die Grossbanken unterhalten spezielle Abteilungen, die ausschliesslich für die Behandlung solcher Geschäfte zuständig sind.

Geradezu klassische Anwendungsbeispiele sind die so genannten Nigeria-Letters⁵⁰. Zu erwähnen sind im Weiteren die Staaten der ehemaligen Sowjetunion, Indonesien, Rumänien, Bulgarien und Zaire.

5. *Hochstaplermodul*

Die handelnden Figuren spiegeln vor, geschäftlich erfolgreich und weltgewandt zu sein. Entsprechend ihres Erfolges sind sie angeblich viel beschäftigt. Ihr Auftreten ist bis ins letzte Detail statusorientiert (Rolex-Armbanduhr, Armani-Anzug, Luxushotel usw.). Das perfekte äussere Auftreten verstärkt die Überzeugungskraft der «deal-story»⁵¹. Die Täter schmücken sich mit akademischen und/oder Adelstiteln. Büroräumlichkeiten werden an bester Lage gemietet, um den Anschein der Seriosität zu unterstreichen. Die Geschädigten lassen sich vor Ort durch die luxuriöse Einrichtung beeindrucken. Vielfach beschäftigen die Betrüger eine grosse Anzahl von Sekretärinnen, welche den Eindruck reger Geschäftstätigkeit erwecken. Auch die Einrichtung einer Sicherheitsorganisation (Bodyguards am Eingang, Überwachungskameras) ist ein oft gesehenes Szenario.

B) **Dokumentenanalyse**

Die Dokumentenanalyse zielt in ihrem Anwendungsbereich auf die Überprüfung der dokumentierten Tätergeschichte. Prioritär soll herausgefunden werden, ob eine Urkunde im weitesten Sinn gefälscht oder verfälscht ist (Fälschungs-

49 *Glinig* (Fn. 8), 150.

50 Darunter wird ein Vorleistungsbetrug verstanden, wobei der Erstkontakt des Opfers schwerwichtig mittels eines unaufgeforderten schemenhaften Briefs resp. E-Mail erfolgt. Auch bekannt unter 419-Fraud: Das nigerianische Strafrecht stellt diese Art von Betrug in Art. 419 unter Strafe.

51 Vgl. *J. W. Coleman*, *The Criminal Elite. Understanding White-Collar Crime*, 4. Aufl., New York 1998, 180 f.; kritisch dazu *Killias* (Fn. 10), 72 ff.

modul)⁵². Selbständige, an der Ausschliesslichkeit der Urkunde orientierte Indikationen sind unwahre Logos (Logo-Modul); auf inhaltliche Unwahrheiten deuten Quasibanktermini (Keyword-Modul) und auffällige, nicht notwendige Ratings (Rating-Modul). Verdachtgewinnungselemente⁵³ sind die unaufgeforderte Zusendung von so genannten Spams (Spam-Modul)⁵⁴ und überflüssige Beglaubigungen der vorgelegten Urkunden (Beglaubigungs-Modul).

1. *Fälschungsmodul*⁵⁵

Das Fälschungsmodul gilt als Anwendungsbeispiel eines materiellen Merkmals. Die Echtheit der Urkunde wird dabei mit investigativen Methoden widerlegt. Kann dieser Beweis geführt werden, steht der Betrugsversuch objektiv fest. Oftmals verwenden Täter Urkunden, auf denen die Firma schlicht falsch geschrieben oder unübliche Zahlenreihen⁵⁶ gebraucht werden. Selbst Adressen, Telefonnummern oder E-Mail-Adressen stellen sich bei Nachprüfung als falsch heraus. In jüngster Zeit kursieren im südostasiatischen Raum Dokumente, die angeblich Urkunden der UBS AG darstellen. Die darauf erwähnte Adresse der Herausgabefiliale in Basel wurde mit *Äschenvorplatz 1, 4052 Basel* angegeben, die Bank befindet sich aber bekanntlich an der *Äschenvorstadt 1, 4051 Basel*.

2. *Logomodul*

Die Finanzbetrüger ahmen bei ihrem Auftritt das Logo von bekannten und renommierten Unternehmungen nach oder verwenden ein bekanntes, veraltetes Logo, welches im Bewusstsein der Öffentlichkeit noch immer an diese Unternehmung erinnert. Verhältnismässig leicht zu überführen sind betrügerische Dokumente der UBS AG, welche aus der Zeit vor 1998 datieren, wenn sie die drei gekreuzten Schlüssel führen, welche vor der Fusion das Logo des Schweizerischen Bankvereins (SBV) waren.

52 S. *Trechsel*, Schweizerisches Strafgesetzbuch, Kurzkommentar, 2. Aufl., Zürich 1997, Art. 251 N 3 f.

53 E. *Kube*, Organisierte Kriminalität: Die Logistik als Präventionsansatz, Ansätze für proaktive Massnahmen, *Kriminalistik* 44 (1990) 632; J. *Ziercke*, Strassenkriminalität. Untersuchung zur Problematik der Verdachtsgewinnung beim ersten Zugriff, *der Kriminalist* 20 (1988) 98.

54 *Fischer* (Fn. 9), 212. Der Autor definiert das «Spam» als eine Werbe-E-Mail, welche der Empfänger unaufgefordert erhält und gleichzeitig in einer grösseren Menge versandt wird.

55 Vgl. auch *Müller/Wabnitz/Janovsky* (Fn. 3), 37: «Unter Einsatz der EDV ist es möglich, Urkunden so zu manipulieren, dass Originale und Fälskate oft nicht mehr unterschieden werden können.»

56 So auch im Chase Manhattan Fall, siehe unter IV.

3. *Keyword-Modul*

Die Betrüger benützen erfahrungsgemäss Pseudofachausdrücke, welche als materielle Kennzeichen gelten. Dieses verbale Instrumentarium überzeugt oftmals auch die so genannte Fachkompetenz, nämlich Banker und Anwälte. Es existieren nota bene mehrere hundert Pseudofachausdrücke⁵⁷. Grundsätzlich werden vier Keyword-Kategorien unterschieden:

- Die Bezeichnung von inexistenten Investitionsformen sind z.B. US Dollar Bonds, Federal Notes, Medium Term Notes oder Blocked Assets Program.
- Die Verwendung von unmöglichen Bank-Transfer-Elementen wie Prime Bank Instruments, Collateral Purchase Orders, Block Funds Deposit.
- Problematische allgemeine Bank-Termini sind OKD (Old Kuwait Dinar), SKR (Safe Keeping Receipt) oder International Banking Day.
- Letztlich ist auf inexistente Bankdokumente hinzuweisen wie Certified Bank Invoice, BPO (Bank Purchase Order) oder Documentary Letters of Credit.

Gelegentlich trifft man auch ganze Sätze an, die als Betrugswarnung erkannt werden müssen (Key sentences). Ein solches betrügerisches Konstrukt findet sich im Wortlaut «the funds for investment must be good, clean funds of non-criminal origin derived from legitimate business». Einige dieser Begriffe werden mittlerweile derart häufig benutzt, dass sie eine eigene Geschichte haben. Dies hat zur Folge, dass selbst Fachleute aufgrund des wiederholten Vorkommens die Sinn- und Bedeutungslosigkeit der Begriffe nicht erkennen.

Zum Keyword-Modul sind ebenso die unpräzisen, grammatikalisch fehlerhaften Formulierungen in Urkunden zu zählen, welche jedoch lediglich als formelle Merkmale aufgefasst werden können. Oftmals wird mit rudimentärem Englisch operiert.

4. *Rating-Modul*

Das Rating ist ein oft gebrauchtes Instrument, um in der Finanzwelt die Kreditwürdigkeit einer Unternehmung zu beurteilen und diese in Relation zur Konkurrenz zu setzen⁵⁸. Dieses Bonitätskriterium machen sich die betrügerischen Anbieter von Finanzgeschäften zu eigen, indem sie fiktive Topratings hinzufügen, um die Glaubwürdigkeit ihrer *deal story* zu erhöhen. Unseriös ist insbesondere, wenn Ratings ohne Agenturnamen gebraucht werden oder für Finanztitel verwendet wer-

57 Wie auch Referenzen auf nicht existente Dokumente der International Chamber of Commerce (ICC). Z.B.: UCP 400 (Uniform Customs and Practices for Documentary Credits).

58 Beispiele: <http://www.standardandpoors.com>; <http://www.moody.com>; <http://www.fitchratings.com>.

den, bei denen sie unüblich sind. In dasselbe Gebiet fällt, wenn die Bank mit ominösen Quasi-Fachausdrücken wie «Top 25 European Bank», «Top 100 Prime Bank», «Escrow Bank» oder «Fiduciary Bank» bezeichnet wird.

5. *Spam-Modul*

Es ist prinzipiell nicht vertrauenserweckend, wenn beim Erstkontakt für ein angeblich lukratives und seriöses Finanzgeschäft unaufgefordert ein Massenwerbemail (Spam⁵⁹) verwendet wird. Das Spam-Mail steht pars pro toto für sämtliche Telekommunikationsmittel, mit welchen der Massenversand möglich ist.

6. *Beglaubigungsmodul*

Ausgehend vom Grundsatz, dass Finanzdokumente auch ohne notarielle Beglaubigung durchaus rechtsgültig sind, zeichnen sich Urkunden betrügerischen Ursprungs dagegen durch eine Vielzahl von Stempeln und notariellen Beglaubigungen aus. Die Beglaubigungen sind jedoch häufig das einzig Echte an der Urkunde und in vielen Ländern leicht erhältlich⁶⁰. Sie sollen den Anschein der Glaubwürdigkeit vermitteln. Ebenso werden ohne Notwendigkeit Bankreferenzen über eine involvierte Figur hervorgebracht. Äusserste Vorsicht ist geboten, wenn die Echtheit des Dokuments speziell betont wird. Trotzdem lassen sich überraschend häufig Opfer dadurch beeindrucken. Auf einer in englischer Sprache verfassten Totalfälschung, einem Papier, das angeblich von der UBS AG stammen soll, fanden sich beispielsweise Stempel mit dem Schriftsatz «Allgemeine Versicherung» nebst einem Phantasiewappen. Solche einfache Beglaubigungsstempel sind materiell entlarvend.

C) **Strukturanalyse**

Die Strukturanalyse zielt in ihrem Anwendungsbereich auf den modus operandi und die Struktur der Tat. Sie beschäftigt sich auch mit den Optionsspektren der Täter. Ausgehend vom Ablaufschema der Tatbegehung untersucht sie vorab den «kriminellen» Kernprozess⁶¹, d.h. das Bündel all jener Tätigkeiten, das darauf

59 Siehe Fn. 54.

60 So auch in den USA, wo Beglaubigungen durch den Public Notary ausgestellt werden.

61 J.-P. Thommen, Managementorientierte Betriebswirtschaftslehre, 6. Aufl., Zürich 2000, 626, wonach ein Kernprozess aus einem Bündel funktionsübergreifender Tätigkeiten besteht, das darauf ausgerichtet ist, einen Kundenwert zu schaffen.

ausgerichtet ist, einen kriminellen Erfolg zu realisieren. Die Module des kriminellen Kernprozesses basieren vor allen Dingen auf einer persönlichen Eigenschaft des Täters, nämlich seiner ausgeprägten Eloquenz. Die Schwindler bedienen sich hervorragender verkaufpsychologischer Methoden. Sie wissen die Opfer einzuwickeln.

Eingangs wird beim Opfer durch ein hohes Gewinnversprechen die Gier geweckt (Highflyer-Modul), die Zweifel des Kontaktierten mit einer speziellen Geschichte (Dealstory-Modul) und/oder einer Pseudoerklärung (Plausibilitäts-Modul) ausgeräumt. Die kritische Frage des Opfers, wieso gerade er kontaktiert wurde, wird mit der Auserwähltheit des Angesprochenen pariert und die Schlusszweifel der getäuschten Person nach dessen Recherche mit einer angeblichen Verschwörung (Konspirations-Modul) ausgeräumt.

Als Supportmechanismen bedient sich der Kriminelle des Zeitdrucks (Zeitdruck-Modul), des zusätzlich karitativen Elements der Transaktion (Wohltätigkeits-Modul) und des historischen, im Internet visualisierten Erfolgs seines Produkts (Internet-Modul).

Nebenimplikationen des Geschäfts sind allenfalls Steuerersparnisse (Illegalitäts-Modul, Absatzkanal-Modul) und das Mitwirken im globalen Markt (Globalitäts-Modul).

1. *Krimineller Kernprozess*

a) *High-Flyer-Modul*⁶²

Als High-Flyer im Sinne des Moduls definiert sich das Versprechen eines aussergewöhnlichen Gewinns (15% p.a. und mehr) bei einer Finanztransaktion, welche beispielsweise damit erklärt wird, dass bei diesem Geschäft mit Grosssummen gehandelt wird. Der Ertrag wird als risikolos und fix garantiert dargestellt. Oftmals wird schon am Anfang ein Folgegeschäft in Aussicht gestellt, welches noch viel höhere Gewinne verspricht. Der vom Opfer zu erbringende Einsatz ist zum zu erwartenden Gewinn tief proportioniert. Opfer und Täter verhalten sich im Grunde genommen unredlich: Das Opfer möchte für «nothing» «something» und der Täter bietet für «something» «nothing». U.E. fällt diesem Modul eine Schlüsselposition zu. Es weckt die Gier des interessierten Anlegers und bezweckt seine Immunisierung gegen unter normalen Umständen vorhandene Zweifel an der Lauterkeit des vorgeschlagenen Geschäfts.

62 Vgl. dazu *M. Glinig*, International Financial Fraud. Bogus Banking: Organised Fraudsters Inflict Billion Dollar Losses, Salzburg 1996, 20 f.

b) *Dealstory-Modul*

Unter *deal story* ist die Gesamtheit der Umstände zu verstehen, aufgrund derer der aussergewöhnlich hohe Gewinn erst plausibel erscheint. Grundsätzlich wird eine besondere Situation, ein Ausnahmefall, kreiert, welche nur erschwert überblickt und kontrolliert werden kann. Häufig wiederkehrende Elemente sind dabei Kriegswirren⁶³, Embargo⁶⁴, Finanzrestriktion, Wirtschaftskrisen⁶⁵, wissenschaftliche Entdeckungen (medizinische Fortschritte)⁶⁶ und Investitionen in Devisen, Goldminen⁶⁷, Bergbau, Rennstrecken⁶⁸ sowie Tourismusprojekte.

c) *Plausibilitätsmodul*

Jeder Anleger möchte sein Geld sicher investiert wissen. Die *deal story* erscheint dem Opfer kompliziert, aber auch professionell. Die Betrüger nützen dabei Unsicherheit und Scham des Opfers über die eigene Unkenntnis resp. das Unvermögen, das Finanzkonstrukt zu durchschauen, aus. Gleichsam sollte die Story so logisch klingen, dass der Anleger nicht in Versuchung kommt, nachzufragen oder gar auf eigene Faust Nachforschungen zu betreiben. Der Anbieter ist mit einer scheinbar einleuchtenden Erklärung zur Stelle, um den Verdacht des Anlegers im Keime zu ersticken. Eine falsche Sicherheit verbreitet auch die Behauptung der Betrüger, dass das investierte Kapital auf einem Sperrkonto (z.B.: Escrow-Account, Treuhandkonto oder Anwaltskonto) verbleibt. Aus irgendwelchen «Zufällen» verschwindet das Geld dann dennoch von diesem Konto.

Als Faustregel gilt hierbei, dass eine Geschäftsidee auf höchstens einer A4-Seite plausibel und verständlich dargestellt werden sollte, damit sie als vertrauenswürdig betrachtet werden kann. Ansonsten sind solche Finanzgeschäfte zu meiden, sofern sie nicht von renommierten Finanzinstituten angeboten werden.

Darüber hinaus operieren die Täter auch mit komplizierten Vertragskonstrukten, welche meist englisch verfasst sind. Sie ergeben auch nach mehrmaligem Lesen keinen Sinn. Die Opfer wagen aus Scham nicht nachzufragen.

63 Z.B.: Kuwaitische Dinars sind angeblich von irakischen Truppen im ersten Golfkrieg erbeutet worden und auf dem Balkan im Rahmen der kriegerischen Auseinandersetzungen wieder aufgetaucht. Diese Devisen sind zu einem einmalig tiefen Kurs angeboten worden.

64 Z.B.: Durch Umgehung des UN-Embargos gegen Libyen.

65 Z.B.: Infolge der Wirtschafts- und Bankkrisen in verschiedenen Staaten Südamerikas werden angeblich Millionenvermögen angeboten für den Bruchteil ihres Wertes.

66 Z.B.: Investitionen in angebliche Krebsheilmittel.

67 Siehe Beispielsfall unter IV.

68 Z.B.: Bevor in Bahrein das heute reelle Projekt einer Formel 1-Rennstrecke an die Hand genommen wurde, waren verschiedene Phantomprojekte gehandelt worden, welche als rentable Investitionen vermarktet wurden.

d) *Konspirationsmodul*

Das Konspirationsmodul ist Fundament der Explikation für die vom Angesprochenen gestellte Frage nach seiner Privilegierung für das angetragene Geschäft. Ausgehend von der Aversion der Öffentlichkeit gegen Banken und Grosskonzerne wird erklärt, dass diese die wahrhaft rentablen Geschäfte selber betreiben und den Durchschnittsbürger davon ausschliessen. Es wird quasi die Konspiration des Grosskapitals gegen den «kleinen Mann» heraufbeschworen. Die Standarderklärung lautet: «*This is the way all banks or big banks make their money.*» (*Auf diese Weise verdienen die grossen Banken ihr Geld.*) Voraussehend macht der Betrüger dem Opfer klar, dass Nachfragen bei der Bank obsolet ist, weil sie solche Geschäfte geheim halten. Dieses Vorgehen ist unter anderem bekannt aus dem Handel mit angeblichen Bankgarantien, der eben nur den Banken vorbehalten sei⁶⁹. Dieser inexistente Markt ist genauso illusorisch wie der Verkauf von alten kuwaitischen Dinars. Der Angesprochene wird bei Abschluss des Geschäftes Teil einer Gegenkonspiration gegen die «Grossen».

2. *Supportmechanismen*

a) *Zeitdruckmodul*

Betrügerische Geschäfte müssen fast immer unter höchstem Zeitdruck abgeschlossen werden. Die Gelegenheit ist an ein konkretes Zeitfenster gebunden. Dahinter steht die Absicht der Reduktion der Kontrolle. Darf für ein Geschäft in Millionenhöhe nicht die branchenübliche Zeit für den Abschluss ausgenutzt werden, ist dieser Umstand zumindest nicht vertrauenserweckend.

b) *Wohltätigkeitsmodul*

An das schlechte Gewissen der Amerikaner und Europäer appellierend wird behauptet, Teile der Einnahmen würden für Sozialprojekte in Afrika⁷⁰, für die kranken und hungernden Kinder verwendet. Die Formel, welche den Opfern vorgetragen wird, lautet: Ein bestimmter Prozentsatz der Anlage muss zwingend für Wohltätigkeitsprogramme bzw. humanitäre Hilfe verwendet werden. Diese Geschäfte sind

69 J. E. Byrne, *The Myth of Prime Bank Investment Scams*, Institute of International Banking Law & Practice, Inc. Third Edition, 2002, 1 ff.

70 Glinig (Fn. 8), 145.

fiktiv. Der Appell an das soziale Gewissen zerstreut eigentlich berechtigte Zweifel der Anleger⁷¹.

c) *Internet-Chart-Modul*

Mit dem Internet-Chart-Modul ist das Phänomen gemeint, wonach die Performance eines Titels (mit oder ohne Passwort) ausschliesslich auf dem Internet kontrollierbar ist. Vertrieb und Bewertung des Titels fallen quasi in einer Hand zusammen. Somit gibt es auch keine unabhängige Marktkontrolle. Dieselben Überlegungen treffen ebenso auf Finanzprodukte zu, welche unter Ausschluss der öffentlichen Kontrolle auf einem einzigen Medium gehandelt werden (z.B. Anlagebriefe). Ein Anwendungsbeispiel ist das Boiler-Room-Phänomen^{72, 73}.

3. *Nebenimplikationen zum Kernprozess*

a) *Absatzkanalmodul*

Der Vertriebskanal von Finanzderivaten läuft grundsätzlich über Banken und Brokerhäuser. Werden solche Titel plötzlich auf ungewöhnlichen Absatzkanälen, beispielsweise auf dem Internet oder durch Privatpersonen, angeboten, muss sich der potenzielle Abnehmer die Frage stellen, wie diese Produkte auf derartige Vertriebskanäle kommen. Diese Frage ist umso berechtigter, wenn gerade «Brand»-Produkte unüblich veräussert werden.

b) *Illegalitätsmodul*

Es besteht ein enger Zusammenhang zwischen Absatzkanal und Legalität der Transaktion. Der Anleger nimmt in Kauf, dass er mit dem vorgeschlagenen Geschäft gegen rechtliche Vorschriften verstösst und verspricht sich dadurch finanzielle Vorteile. In Betracht kommen dabei unrechtmässiges Erwirken von Steuervorteilen und das Umgehen der Geldwäschereigesetzgebung. Ungewöhnliche Absatzkanäle, wie oben beschrieben, sind dabei für den Anleger sehr attraktiv, was ihn für deliktische

71 Vgl. auch zum Schenkungs- oder Bettelbetrug: A. Donatsch, Betrug durch Zweckentfremdung von arglistig erlangten Vermögensleistungen, in: Festschrift für Niklaus Schmid, Wirtschaft und Strafrecht, hrsg. von J.-B. Ackermann/A. Donatsch/J. Rehberg, Zürich 2001, 278.

72 Ebenso illustrativ das Beispiel in: FACTS Nr. 16 vom 19. April 2001, 64 f.

73 Unter *boiler rooming* ist das gezielte Hochtreiben eines Titels und dessen anschliessender manipulativer Kurssturz unter Abschöpfung des Kursgewinns zu verstehen; siehe auch *Glinig* (Fn. 8).

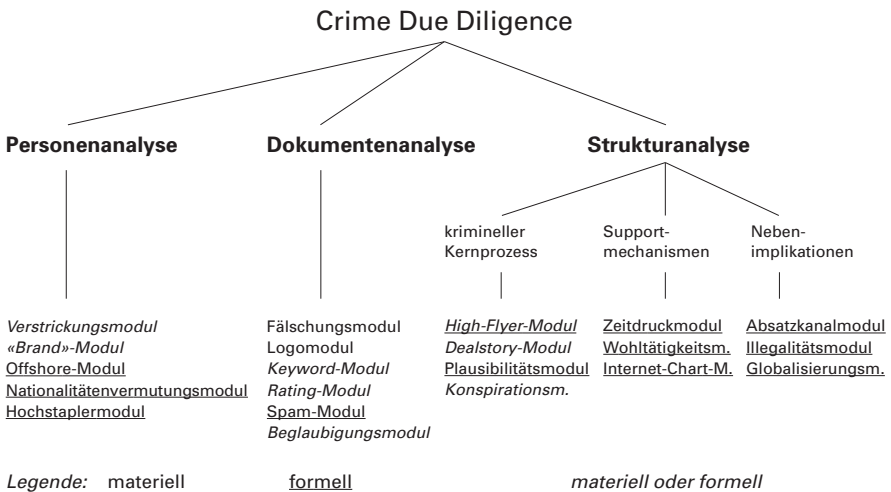
Finanzgeschäfte sehr empfänglich macht. Diesbezüglich gilt es auf die bemerkenswerte bundesgerichtliche Rechtsprechung in BGE 124 II 58 ff. hinzuweisen. Dieser Entscheid stellt sinngemäss die Vermutung auf, dass, wenn jemand eine hoch spekulative Anlagestrategie verfolge, er dies a priori mit hinterzogenem, also steuerneutralem Geld tue.

Illegal ist auch, wenn der Anleger versucht, Embargos gegen bestimmte Staaten zu umgehen oder Devisen-Restriktionen zu verletzen.

c) *Globalisierungsmodul*

Das Globalisierungsmodul kommt zur Anwendung, wenn eine Finanztransaktion über Staaten läuft, welche in dieser Zusammensetzung keinen wirtschaftlich nachvollziehbaren Sinn ergeben. Zwar kommen bei internationalen Geschäften zwangsläufig mehrere Staaten ins Spiel. Nicht einsichtlich ist aber zum Beispiel, weshalb Goldminenzertifikate aus Kanada unbedingt in der Schweiz und nicht vor Ort in Kanada behelnt werden sollen⁷⁴. Ähnlich gelagert ist der Fall, wenn in der Schweiz ein chinesisches Wertpapier angeboten wird, mit welchem in Indonesien Autobahnen finanziert werden sollen.

D. **Übersichtsschema**



74 Siehe Goldminen-Fall unter 4.

VI. Anwendbarkeit der Analysen

Die Analysen können nicht schablonenhaft angewendet werden. Sofern nicht ein materielles Crime Due Diligence-Ergebnis vorliegt, sind die jeweilig zutreffenden Modulkombinationen differenziert zu bewerten. Beispielsweise ist durchaus denkbar, dass eine Finanzoperation nur im Internet einzusehen ist (Internet-Chart-Modul), auf einem Offshore-Finanzplatz stattfindet (Offshore-Modul) und unter höchstem Zeitdruck zu erfolgen hat (Zeitdruckmodul); dennoch kann in einem derart gelagerten Fall nicht per se von einem deliktischen Hintergrund gesprochen werden. Die Bewertung der im zu überprüfenden Geschäft anwendbaren Module basiert einerseits auf Erfahrungswerten und andererseits auf Gewichtungskriterien (z.B. materiell vor formell). Die nachfolgend erläuterten Fälle, welche sich n.b. wirklich zugetragen haben, sollen das beschriebene Prinzip illustrieren:

1. Fallbeispiel: Im Jahre 2001 wandte sich eine Investmentfirma aus Marbella (ESP) mittels einer Telefon- und Faxkampagne an verschiedene Anleger. Die Firma hatte ein Off-Shore-Domizil in Gibraltar und trug den Namen «Capital Swiss». Auf dem professionell aufgemachten Briefpapier fand sich ein Logo, das jenem der Credit Suisse täuschend ähnlich schien. Erwiesenermassen war auch eine bekannte, sehr renommierte schweizerische Privatbank Kunde der Capital Swiss und liess mehrere Millionen CHF durch die fragliche Firma verwalten. Capital Swiss versprach eine Jahresrendite von bis zu 50%. Im Jahre 2001 hatte sie verschiedenen Anlegern unbestreitbar eine solch hohe Rendite ausbezahlt, was diese wiederum bewog, mit noch grösseren Beträgen einzusteigen. Als Referenz verwies Capital Swiss auch auf einen kantonalen Notariatsverband aus der Schweiz, der tatsächlich ebenfalls Kunde des Finanzinstituts war.

Die praktische Anwendung der Crime Due Diligence förderte das Spam-Modul, das Offshore-Modul, das Logomodul, das Beglaubigungsmodul sowie das High-Flyer-Modul zu Tage. Insgesamt lag eine klare Indikation für den kriminellen Hintergrund vor. Leider bemerkten dies viele geprellte Anleger zu spät.

2. Fallbeispiel: Im Jahre 1998 wandte sich die EMG (Equity Management Group) telefonisch an verschiedene potenzielle Anleger in Europa, insbesondere in der Schweiz, in den USA und Asien. Sie sandte den kontaktierten Personen eine Hochglanz-Dokumentation zu, die unter anderem im Logo einen goldprägten Globus enthielt. Die Firma verfügte über ein Postfach in Nassau auf den Bahamas und war dort auch domiziliert. In der Folge wechselte die EMG zweimal ihr Domizil und firmierte auf anderen Offshore-Plätzen. Sie versprach den Anlegern grösse Gewinn und nahm auch kleinere Investitionskapitalien entgegen. Die Anleger konnten sich laufend auf einer hochprofessionellen Website⁷⁵ über die Erfolgsge-

75 <http://www.equitymgmtgrp.com>.

schichte der von ihnen erworbenen Titel informieren. Die Investoren erhielten zudem regelmässig Schreiben⁷⁶, in welchen ihnen die überdurchschnittliche Titelperformance bestätigt wurde. Der Durchschnittsanleger erzielte pro Halbjahr ca. 40% Rendite.

In diesem Fall erfüllten sich das Spam-Modul, das Hochstaplermodul, das Logomodul, das Offshore-Modul und das High-Flyer-Modul. Die Crime Due Diligence ergab ebenfalls ein klares Resultat: Diese Finanzanlage verfolgte mit hoher Wahrscheinlichkeit einen deliktischen Erfolg.

VII. **Schlussbemerkung**

Die Wirtschaft wusste die Rahmenumstände, welche die technische Entwicklung und der weltweite schrankenlose Einsatz der Computer- und Informationstechnologie gebracht haben, umgehend zu adaptieren⁷⁷. Wie bei jeder technischen Revolution, die das Leben der Menschheit nachhaltig verändert, versucht das Verbrechen, die neuen Möglichkeiten für seine Zwecke zu missbrauchen. Nachdem die Tätererkennung dadurch schwieriger geworden ist, erhält jedermann, vom einfachen Kleinanleger bis zum professionellen Strafverfolger, in Form der Crime Due Diligence ein Instrument, welches die Tat(früh)erkennung ermöglicht. Die Jägerschen Schemen, das Profiling und die Rasterfahndung greifen erst nach Tatverübung ein. Crime Due Diligence hingegen wirkt einerseits präventiv, indem sie vor Vollendung der Tat einsetzt. Andererseits liegt ihre Wirkung ebenso auf der Repressionsebene. Die Crime Due Diligence entfaltet dabei ihre Wirkung gleich auf mehreren Ebenen. Sie unterstützt sowohl die Strafverfolgungsbehörden bei der Deliktsaufdeckung wie auch die richterlichen Behörden bei der Urteilsfindung. Einen gravierenden Nachteil der Strafverfolgung im Zeitalter des grenzenlosen World Wide Webs vermag jedoch auch sie nicht zu beseitigen: Das Territorialitätsprinzip behindert nach wie vor die effektive Verfolgung. Letztlich eröffnet die Crime Due Diligence dem spezialisierten Rechtsanwalt ein neues Tätigkeitsfeld, indem er in seiner beratenden Tätigkeit verbrechensverhindernd handeln kann.

76 Schreiben, die dem Anleger eine hohe Rendite bestätigen, heissen im Fachjargon auch «Good-feel-Letters».

77 Müller/Wabnitz/Janovsky (Fn. 3), 37.