

2.5 Crime Due Diligence – ihre Bedeutung für Gesellschaftsorgane



Prof. Dr. Daniel Fischer

Der Autor

Daniel Fischer wurde 1953 in Bern geboren. Er studierte in Bern Rechtswissenschaft und beendete in der Folge dieses Studium 1979 mit dem Rechtsanwaltsdiplom.

1979 eröffnete er eine Anwaltskanzlei in Bern, später kamen die Kanzleien in Zürich und Zug dazu, welche alle unter Advokaturbüro Fischer & Partner firmieren. Die Kanzleien arbeiten national und international mit dem Schwerpunkt Wirtschafts- und Wirtschaftsstrafrecht.

Daniel Fischer ist Titularprofessor und Lehrbeauftragter. Er entwickelt den Terminus «Econ Crime», anstelle von «White Collor Crime», sowie die Instrumente der Crime Due Diligence und des Delinquenz Risk Managements. Hierfür unterhält er auch eine Hotline +41 1 482 70 23. Er ist Certified Fraud Examiner und Trainingsdirektor dieser Organisation in der Schweiz.

Beachtung fanden seine Vorträge im Jahre 2003 am Swiss-Re-Kongress in Zürich sowie am europäischen Betrugskongress im Oktober 2004 in London.

In den letzten zwei Jahren publizierte er die folgenden Aufsätze:

- Die Gefährdung der Unternehmensfinanzen durch New Econ Crime, in Finanz- und Rechnungswesen, Prof. Dr. H. Siegwart, Jahrbuch 2003
- Crime Due Diligence, eine Verdachtschöpfungsstrategie, in Zeitschrift für Strafrecht, Band 121, Heft 2, 2003,
- New Econ Crime und New Economy, in Meilensteine im Management, Band 10, Management & Law, Hrsg.: H. Siegwart/ J. Mahari, Basel 2003
- Der Richter und sein Gutachter: die strafrechtliche Verantwortung des Gutachters, in: Die neurologische Begutachtung, by Orell-Fuessli, Co-Autor, 2004
- Ferienwohnung und Recht, in Newsletter Swissapartments, 2004

Inhalt

1. Problemstellung.....	3
2. Begriff der Crime Due Diligence	5
3. Analysen	7
4. Anwendbarkeit der Analyse.....	11
5. Schlussbemerkung.....	12

Crime Due Diligence – ihre Bedeutung für Gesellschaftsorgane¹

1. Problemstellung

Der Gesetzgeber wie auch die Gerichtspraxis sind heute bestrebt, die Organe der juristischen Personen verstärkt in die rechtliche Verantwortung einzubinden. Die Art. 100^{quater} und Art. 100^{quinquies} CHStGB² unter dem Titel Verantwortlichkeit des Unternehmens³ stellen eine Novität im Gebiet des Strafrechts dar, worin in Durchbrechung des eisernen Grundsatzes «societas delinquere non potest» eine direkte strafrechtliche Haftung des Unternehmens bis zu einer Busse von CHF 5 Mio.⁴ statuiert wird, wenn «in Ausübung geschäftlicher Verrichtungen im Rahmen des Unternehmenszwecks» eine Straftat begangen wird und diese wegen mangelhafter Organisationsstruktur keiner bestimmten natürlichen Person zugerechnet werden kann. Deshalb ist es notwendig, dass sich die höchsten Organe der Unternehmen – in ihrem ureigensten Interesse – dem Problemkreis der Verhütung von Delinquenzfällen in den eigenen Reihen zuwenden. Ein Blick über die Grenzen nach Deutschland⁵ zeigt, dass die Diskussion um die Verbandsstrafbarkeit ebenfalls eingesetzt hat⁶. De lege lata existiert jedoch noch kein vergleichbarer Straftatbestand im Deutschen Recht.

- 1) Meinem juristischen Mitarbeiter Rechtsanwalt lic. iur. Pascal Honold, Zürich, danke ich für die Unterstützung beim Verfassen dieses Beitrags.
- 2) Mit der Gesetzesnovelle vom 21. März 2003 (Bundesgesetz über die Änderung des Strafgesetzbuches und des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs [Finanzierung des Terrorismus], AS 2003 3043) sind diese Bestimmungen neu in Kraft getreten. Vgl. dazu EIDAM, GERD, Unternehmen und Strafe, 2. Aufl., Köln 2001.
- 3) In Österreich soll per 1.1.2005 das Bundesgesetz über die Verantwortlichkeit von Verbänden für mit gerichtlicher Strafe bedrohte Handlung, das Verantwortlichkeitsgesetz (VbVG), in Kraft treten.
- 4) In Österreich basiert die Bussenbestimmung auf einem Ertragsäquivalent in der Höhe von 0,0005% bis 0,01% des Jahresumsatzes, wobei diese Einheit 1500 Mal bei der Bemessung verhängt werden kann.
- 5) Zahlreiche Rechtsakte der EU verpflichten die Mitglied- oder Vertragsstaaten, eine Verantwortlichkeit juristischer Personen für bestimmte Straftaten vorzusehen. Erstmals geschah dies in der EU mit dem zweiten Protokoll vom 9.6.1997 zum Übereinkommen über den Schutz der finanziellen Interessen der Europäischen Gemeinschaft.
- 6) FISCHER, THOMAS, Beck'sche Kurz-Kommentare, Band 10, Strafgesetzbuch und Nebengesetze, 52. Aufl., München 2004, N 1c zu § 14.

Zu dieser gesellschaftlichen Entwicklung kommen revolutionäre Veränderungen im Wirtschaftsleben und in dessen Fahrwasser eine neue Dimension von Wirtschaftsdelikten. In der Lehre werden sie einerseits immer noch mit Wirtschaftskriminalität⁷ oder «White collar crime»⁸ bezeichnet, andererseits sind aber auch neue Termini wie unter anderem Finanzbetrug⁹ oder EconCrime¹⁰ geläufig¹¹. Es wurde zudem festgestellt, dass sich in den letzten Jahren die Delikte gegen die Wirtschaftsgüter nicht nur quantitativ sondern auch qualitativ, sozusagen in ihrem Kern, verändert haben¹². Diese Entwicklung ist im Wesentlichen auf zwei Faktoren zurückzuführen:

- Zum einen beschleunigt die Informationsdigitalisierung den Wirtschaftshandel erheblich. Gleichzeitig wurde er anonym und grenzüberschreitender. Dies erlaubt es, Delikte weitaus effizienter, in einem bis anhin ungeahnten Ausmass und ebensolcher Geschwindigkeit zu begehen¹³.
- Zum anderen sind institutionelle wie auch Privat-Geldanleger mit ständig zahlreicheren, vielfältigeren, zuweilen auch sehr komplizierten Investitionsformen auf dem Finanzmarkt konfrontiert. Dabei die Übersicht und den Durchblick zu bewahren, erscheint heute selbst für Anlageexperten beinahe unmöglich.

7) BOERS, KLAUS: Wirtschaftskriminologie. Vom Versuch, mit einem blinden Fleck umzugehen, Monatsschrift für Kriminologie und Strafrechtsreform, Heft 5 (2001), S. 335, wonach die kriminologische Forschung zur Wirtschaftskriminalität von jeher mit begrifflichen, methodischen und theoretischen Schwierigkeiten konfrontiert ist.

8) SUTHERLAND, EDWIN H.: White Collar Crime. The uncut version. With an introduction by Gilbert Geis and Colin Goff, New Haven/London 1983, S. 7: «White Collar Crime is a crime committed by a person of respectability and high social status on the course of his occupation».

9) GLINIG, MANFRED: Der internationale Finanzbetrug, 3. Aufl., Wien 2000, S. 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.

10) FISCHER, DANIEL: in: SIEGWART, HANS (Hrsg.), Finanz- und Rechnungswesen, Jahrbuch 2003, Zürich 2003, S. 208; unter Econcrime versteht der Autor die Verursachung von Schaden durch Verletzung rechtlich geschützter Wirtschaftsgüter, in erster Linie durch den Gebrauch bestimmter Technologien und/oder durch die Verwendung von Sachkenntnis, wobei mit verhältnismässig tiefen Kosten ein hoher Schaden verursacht wird. Detaillierter: FISCHER, DANIEL in: Schweizer Zeitschrift für Strafrecht Band 121, 2003, Heft 2, S. 216 ff. und FISCHER, DANIEL in: Siegwart Finanz und Rechnungswesen 2003, S. 208 ff.

11) KILLIAS, MARTIN: Von «White Collar Crime» zur organisierten Kriminalität: Zeitgenössische Inkarnation des Bösen, in: FS für Niklaus Schmid zum 65. Geburtstag, Wirtschaft und Strafrecht, ACKERMANN, JURG-BEAT/DONATSCH, ANDREAS/REHBERG, JÖRG (Hrsg.), Zürich 2001 S. 71 ff.

12) DANNECKER, GERHARD: in: WABNITZ, HEINZ-BERND/JANOVSKY, THOMAS (Hrsg.), Handbuch des Wirtschafts- und Steuerstrafrechts, München 2000, S. 6.

13) So auch MÜLLER, RUDOLF/WABNITZ, HEINZ-BERND/JANOVSKY, THOMAS: Wirtschaftskriminalität. Eine Darstellung der typischen Erscheinungsformen mit praktischen Hinweisen zur Bekämpfung, 4. Aufl., München 1997, S. 37: «Die technische Entwicklung und der weltweite schrankenlose Einsatz der Computer- und Informationstechnologie hat die nationalen Gesetzgeber [...], insbesondere die Ermittlungsbehörden überrollt.»

Die vorbeschriebene Ausgangslage wird von raffinierten Schwindlern ausgenutzt, welche durch ausgeklügelte Vorgehensweisen und überlegene Kommunikation die Opfer übertölpeln. Es müssen ihnen darum neue Erkennungsmethoden entgegengesetzt werden, welche die Informationsdigitalisierung und Anonymität der Kapitalwirtschaft berücksichtigen.

Im wesentlichen Unterschied zu früher sind die bevorzugten Opfer nicht mehr nur die einfachen Bürger und ihr Sparschwein sondern dank den modernen technologischen Möglichkeiten insbesondere auch Unternehmen, Gross- und Kleinbetriebe. Die Organe¹⁴ der Gesellschaft sind deshalb besonders gefordert. Es geht dem Autor in diesem Artikel darum, die Verantwortungsträger auf die neuen Gefahren hin zu sensibilisieren und geeignete Verhaltensmuster in Krisensituationen aufzuzeigen.

Frei nach George Washington, der gesagt haben soll: «Kleine Ausgaben am Anfang ersparen grosse Ausgaben zum Schluss.»

2. Begriff der Crime Due Diligence

Die Voraussetzung des Erkennens beziehungsweise des Aufdeckens eines Verbrechens ist der Verdacht. Der intuitiven Verdachtsschöpfung¹⁵ 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. Der Täter spielt dabei bewusst mit der Gier und Unwissenheit des Opfers. Dieser Aufsatz handelt insbesondere von Erkennungsstrategien gegen unterschiedlichste Täuschungsszenarien, die – allgemein gesprochen – darauf abzielen, die Täter auf Kosten der Opfer zu bereichern.

Um der gesetzlichen Organhaftung für Verwaltungs- resp. Aufsichtsräte im heutigen Wirtschaftsumfeld adäquat Rechnung zu tragen, bedarf es im Rahmen einer geplanten Finanzoperation 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.

14) Fürs Schweizerische Recht: «Organe sind Personen, die in einer Gesellschaft selbständige Entscheide treffen können oder die eigentliche Geschäftsführung besorgen und so die Willensbildung der Gesellschaft massgebend mitbestimmen.» FORSTMOSER, PETER, MEIER-HAYOZ, Arthur, NOBEL PETER, Schweizerisches Aktienrecht, Bern 1996, § 19 N 10, S. 174; ebenso im Deutschen Recht: Creifelds Rechtswörterbuch, 13. Aufl., München 1992.

15) STÖRZER, UDO: in: KUBE, EDWIN/STÖRZER, UDO/TIMM, KLAUS, JÜRGEN (Hrsg.), Kriminalistik, Handbuch für Praxis und Wirtschaft, Band 1, Stuttgart/München/Hannover/Berlin/Weimar 1992, S. 430.

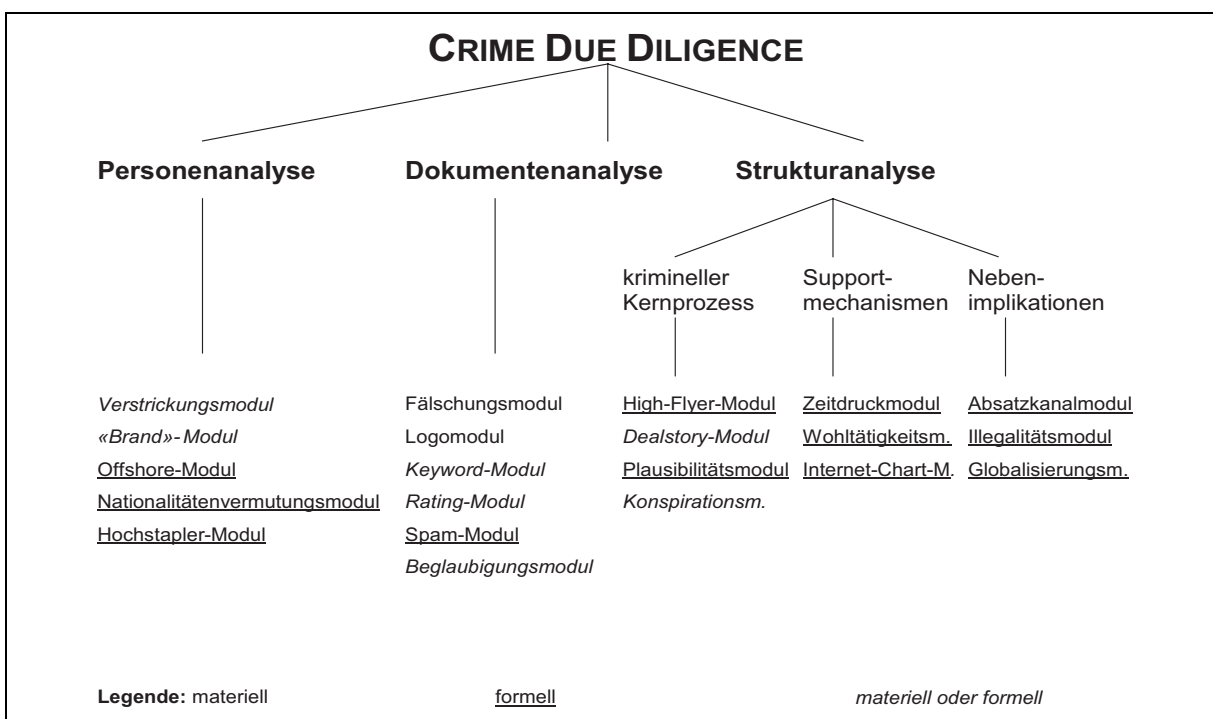
Dieser beruht einerseits auf Erkenntnissen der Fahndungsbehörde und andererseits auf der konkret vorgetragenen und/oder dokumentierten «Tatgeschichte».

Die Analysen werden mit Hilfe von so genannten Modulen vorgenommen. Grundsätzlich treten in einem Verdachtsfall selten alle Module gemeinsam in Erscheinung. Die Taterkennung beruht auf der Bewertung der unterschiedlichen, erkennbaren Module.

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

Grundsätzlich können die Module in *materielle und/oder formelle Komponenten* unterteilt werden. Die materiellen Merkmale haben unmögliche oder erwiesenermassen unwahre Sachverhalte (z.B. inexistente Person involviert) zum Inhalt, wohingegen sich formelle Anhaltspunkte an formal-äusserlichen Kennzeichen (z.B. dubiose Briefkastenfirmaadresse) orientieren¹⁶.

Übersichtsschema¹⁷



16) FISCHER, DANIEL (Fn. 10), S. 216 ff.

17) zum Ganzen: FISCHER, DANIEL (Fn. 10), S. 216 ff.

3. Analysen

3.1 Personenanalyse

Die Personenanalyse zielt in ihrem Anwendungsbereich auf die handelnde Täterpersönlichkeit bzw. die darin involvierten Handlungsfiguren. Diese ist bei betrügerischen Vorgängen absolut entscheidend. Die Täter wissen um die Gefährlichkeit der Aufdeckung ihrer Identität. Sie verwenden deshalb erfahrungsgemäss zwei übliche Schutzszenarien. Einerseits wechseln sie bewusst die Schreibweise ihres Vor- und Nachnamens, dabei die Erkenntnis ausnützend, dass Datenbanken nur Resultate liefern, wenn die korrekte Schreibweise eingegeben wird. Andererseits bleiben die Täter im Hintergrund und schieben möglicherweise nichtsahnende Personen vor. So ist der «Frontman»¹⁸ als jene Person bekannt, die offiziell als Verantwortlicher eines kriminellen Unternehmens figuriert. «Goofer»¹⁹ und «Runner»²⁰ verüben hingegen untergeordnete Tätigkeiten im kriminellen Netzwerk. Ein wichtiger Bestandteil des Netzwerks ist der so genannte «Finder»²¹, der einzig die Aufgabe hat, Opfer ausfindig zu machen und sie zu überzeugen.

Die Personenanalyse untersucht vorab die involvierten Personen, seien diese natürlicher oder juristischer Art.²² Darunter wird einerseits das Aufdecken des Verstrickungszusammenhangs des Zielobjekts oder von Figuren aus dessen Umfeld verstanden, die in anderen Zusammenhängen bei unlauteren Transaktionen bereits negativ in Datenbanken vermerkt worden sind (Verstrickungsmodul): Ein zusätzliches Verdachtsschöpfungsmoment ist die schwierige Identifizierbarkeit einer Person. Vielfach wird versucht, das Vertrauen des Opfers zu erschleichen, indem Passkopien vorgewiesen werden und/oder Personen zusammen mit ihrer Passdokumentnummer auftreten. Dabei ist zu bedenken, dass Passkopien ohne weiteres gefälscht und Passdokumentnummern erfunden werden können oder deren Geschäftssitz (Offshore-Modul) Verdacht erweckt bzw. deren Zugehörigkeit zu verdächtigen Staaten (Nationalitäten-Modul). Die Personenanalyse orientiert sich damit an konkreten Zielvorgaben. Sie beschäftigt sich aber andererseits abstrakt mit jenen Decknamen, welche die Täter prioritär gebrauchen (Brand-Modul) und mit generellen Verhaltensmustern solcher Täter (Hochstapler-Modul).

18) Definition bei GLINIG (Fn. 9), S. 154: gegen aussen als Verantwortlicher auftretend.

19) Definition bei GLINIG (Fn. 9), S. 154: Laufbursche zur Besorgung untergeordneter Tätigkeit.

20) Definition bei GLINIG (Fn. 9), S. 154: Laufbursche zur Besorgung untergeordneter Tätigkeit.

21) Definition bei GLINIG (Fn. 9), S. 154: Krimineller, der die Opfer ausfindig macht und gegen Provision weitervermittelt.

22) Ist eine Firma sehr jung mit einer schwachen Eigenkapitaldecke, ist dieser Umstand zumindest prüfenswert.

3.2 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 (Fälschungsmodul)²³. Auffällig ist in diesem Zusammenhang insbesondere, wenn in Geschäftsverträgen Vertragsparteien immer wieder anders bezeichnet werden. Verträge, welche die Klausel «according to ICC 500» enthalten, sind vorweg verdächtig, weil das Reglement ICC 500 laut International Chamber of Commerce nicht existiert, die Publikation 500 der Internationalen Handelskammer hingegen schon. 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). Verdachtsgewinnungselemente²⁴ sind die unaufgeforderte Zusendung von so genannten Spams (Spam-Modul)²⁵ und überflüssige Beglaubigungen der vorgelegten Urkunden (Beglaubigungs-Modul).

Von entscheidender Bedeutung ist innerhalb der Dokumentenanalyse das Keyword-Modul, welches grundsätzlich in vier Kategorien unterschieden werden kann:

- Die Bezeichnung von inexistenten Investitionsformen wie z.B. «Bank Depenture Program», «Bank Instrument Trading», «Senior Dept Instruments».
- Die Verwendung von unmöglichen Bank-Transfer-Elementen wie «Cash Wire Transfer», «Conditional SWIFT», «Blocked Funds Letter», «Debenture Instruments».
- Problematische allgemeine Bank-Termini sind «Fiduciary Bank», «Money Centre Bank», «Cutting Bank», «Closing Bank».
- Letztlich ist auf inexistente Bankdokumente hinzuweisen, wie «Prime Bank Guarantees», «Zero Coupon L/C», «Proof of Product».

23) Trechsel, Stefan: Schweizerisches Strafgesetzbuch, Kurzkommentar, 2. Aufl., Zürich 1997, N 3 f. zu Art. 251 StGB.

24) KUBE, EDWIN: Organisierte Kriminalität: Die Logistik als Präventionsansatz, Ansätze für proaktive Massnahmen, Kriminalistik 44 (1990), S. 632; ZIERCKE, JÖRG: Strassenkriminalität. Untersuchung zur Problematik der Verdachtsgewinnung beim ersten Zugriff, der kriminalist 20 (1988), S. 98.

25) FISCHER, DANIEL (Fn. 7), S. 212. Der Autor definiert das «Spam» als eine Werbe-E-Mail, welche der Empfänger unaufgefordert erhält und die gleichzeitig in einer grösseren Menge versandt wird.

Gelegentlich trifft man auch ganze Sätze an, die als Betrugswarnung erkannt werden müssen (Key sentences)²⁶. 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». Diese Klausel oder einige der genannten Begriffe werden mittlerweile derart häufig benutzt, dass sie eine eigene Geschichte haben. Das hat zur Folge, dass selbst Fachleute aufgrund des wiederholten Vorkommens die Sinn- und Bedeutungslosigkeit der Begriffe nicht erkennen. Ebenso sind unpräzise, grammatikalisch fehlerhafte Formulierungen in Urkunden dazu zu zählen. Oftmals wird mit rudimentärem Englisch operiert.

3.3 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» Kernprozess²⁷, d.h. das Bündel all jener Tätigkeiten, das darauf 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 Kriminellen bedienen sich hervorragender verkaufpsychologischer Methoden. Sie wissen die Opfer einzuwickeln.

Eingangs wird beim Opfer durch ein hohes Gewinnversprechen²⁸ die Gier geweckt (High-flyer-Modul), die Zweifel des Kontaktierten mit einer speziellen Geschichte (Dealstory-Modul)²⁹ 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 auf das Opfer (Zeitdruck-Modul), des zusätzlich karitativen oder religiösen Elements der Transaktion (Wohltätigkeits- und Religions-Modul) und des historischen, im Internet visualisierten Erfolgs seines

26) In den Vertragstexten betrügerischer Operationen findet sich fast immer eine Geheimhaltungsklausel. Eine solche ist nur in Verbindung mit anderen Hinweisen relevant. Diese Klauseln stehen auch mit dem Konspirationsmodul im Zusammenhang

27) THOMMEN, JEAN-PAUL: Managementorientierte Betriebswirtschaftslehre, 6. Aufl., Zürich 2000, S. 626, wonach ein Kernprozess aus einem Bündel funktionsübergreifender Tätigkeiten besteht, das darauf ausgerichtet ist, einen Kundenwert zu schaffen.

28) Ein Anreiz ist häufig auch, dass diese Anlage steuerfrei oder steuerprivilegiert ist.

29) Ein ähnlicher Denkansatz im Sinne der Klassifizierung von Ereignissen sind die so genannten Krisenfamilien. Siehe in: I.I. Mitroff und C.M. Pearson, *Crisis Management*, 1993, S. 10–45.

Produkts (Internet-Chart-Modul). Die Supportmechanismen haben für das Gelingen der Täuschung lediglich zudienenden Charakter, welche den eigentlichen Kerngehalt der betrügerischen Geschichte bekräftigen, katalysieren oder glaubhafter machen sollen. Das Schweizerische Strafgesetzbuch spricht in diesem Zusammenhang vom qualifizierenden Arglistelement des Betrugs (Art. 146 CHStGB). Im Vergleich dazu kennt das Deutsche Strafgesetzbuch diese Qualifikation im Betrugstatbestand von § 263 Abs. 1 DStGB nicht. Betrügerisches Verhalten setzt eine strafrechtlich relevante Täuschung voraus, welche jede beliebige Handlung darstellen kann, die einen Erklärungswert hinsichtlich Tatsachen besitzt und auf die Vorstellung einer anderen natürlichen Person derart einwirkt, dass sie zu einem Irrtum, d.h. zu einer objektiv fehlerhaften Annahme bezüglich Vorliegen oder Nichtvorliegen dieser Tatsachen führt. Ein subjektives Element enthält die Täuschung nicht³⁰.

Nebenimplikationen des Geschäfts sind zusätzliche Warnsignale, welche das Opfer aufhorchen lassen. Werden Finanztitel plötzlich auf ungewöhnlichen Absatzkanälen, beispielsweise auf dem Internet oder durch Privatpersonen, angeboten statt über Bankhäuser oder Finanzgesellschaften, muss sich der potenzielle Abnehmer die Frage stellen, wie diese Produkte in derartige Vertriebskanäle gelangen (Absatzkanalmodul)³¹. Der Anleger nimmt billigend in Kauf, dass er mit dem vorgeschlagenen Geschäft gegen rechtliche Vorschriften verstösst, und verspricht sich dadurch finanzielle Vorteile (Illegalitäts-Modul). 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 Finanzgeschäfte sehr empfänglich macht. Diesbezüglich gilt es auf die bemerkenswerte Rechtsprechung des Schweizerischen Bundesgerichts in BGE 124 II 58 ff. hinzuweisen. Dieser Entscheid stellt sinngemäss die Vermutung auf, dass, wenn jemand eine hochspekulative Anlagestrategie verfolge, er dies mit hinterzogenem, also steuerneutralem Geld tue. Die Deutsche Praxis kennt keine ähnlich gelagerte Rechtsprechung. Zwar kommen bei internationalen Geschäften zwangsläufig mehrere Staaten ins Spiel. Das Globalisierungs-Modul ist aber dann angezeigt, wenn eine Finanztransaktion über Staaten läuft, welche in dieser Zusammensetzung keinen wirtschaftlich nachvollziehbaren Sinn ergeben. Beispielsweise wird in der Schweiz ein chinesisches Wertpapier angeboten, mit welchem in Indonesien Autobahnen finanziert werden sollen.

30) FISCHER, THOMAS (Fn. 6), N 10 zu § 263.

31) Ungewöhnlichen Werbemethoden muss mit zurückhaltung begegnet werden.

4. Anwendbarkeit der Analysen

Die drei Analysen können nicht schablonenhaft angewendet werden. Sofern nicht ein materielles Element bei der Crime Due Diligence resultiert, sind die jeweils zutreffenden Modulkombinationen differenziert zu bewerten. Beispielsweise ist durchaus denkbar, dass eine Finanzoperation nur im Internet einsehbar 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). Der nachfolgend erläuterte Fall aus der Praxis soll das beschriebene Prinzip illustrieren:

Fallbeispiel

Am 25. August 2000 erschien auf dem News-Dienstleister Internet Wire eine wahrheitswidrige Meldung über das Hardware-Unternehmen Emulex Cooperation, USA³². Die Verlautbarung kündete einen Umsatzeinbruch an, welcher von der Securities and Exchange Commission (SEC) untersucht werde, und dass der CEO deshalb zurücktrete (im Originaltext: «Emulex Announces Revised Earnings; SEC Launches Investigation Into Accounting Practices. Paul Folino Steps Down As CEO.»). Reputierte Presseagenturen wie Bloomberg und Reuters nahmen das Communiqué von Internet Wire ungeprüft auf und publizierten es, woraufhin der Aktienkurs von Emulex um fast 60% von 113,06 US\$ auf 43 US\$ einbrach. Es stellte sich im Nachhinein heraus, dass die Meldung von Mark S. Jakob, einem in gekündigter Stellung arbeitenden Mitarbeiter, wohl aus Rache verfasst und per Internet verbreitet worden war. Als kleiner Nebeneffekt verdiente dieser sich 200 000.– US\$, indem er seine Emulex-Aktien unmittelbar nach dem Crash des Aktienkurses handelte. Nachdem Emulex die Falschmeldung hatte richtig stellen können, erholte sich der Aktienkurs etwas, erreichte aber den Stand von vor dem Crash nicht mehr. Der Schaden trat vor allem bei den Investoren ein, welche die Aktien unmittelbar nach der Pressemitteilung in Panik verkauften. Die Schadenssumme belief sich schätzungsweise auf 110 Millionen US\$ wegen des Kurseinbruches an der Börse. Eine Chance, ihr Geld wiederzuerlangen, bestand für die Aktionäre nicht, weil Presseagenturen nicht für die Richtigkeit ihrer Meldungen haften (Disclaimer) und der Schädigende nicht vermögend war. Gleichwohl wurde der Schädigende strafrechtlich zur Rechenschaft gezogen.

32) MANN, BILL, in: The Motley Fool, 2000, Arrest Made on Emulex Case.

Angenommen, der Verfasser der Falschmeldung hätte im beschriebenen Fall unerkannt bleiben können, hätte dies für die obersten Organe der Emulex Cooperation ebenfalls strafrechtliche Konsequenzen haben können. Nach dem neu eingeführten Art. 100^{quater} CHStGB kann das Unternehmen mit einer Busse von bis zu CHF 5 Mio. belegt werden. Der Verwaltungs- resp. Aufsichtsrat hätte mit Bestimmtheit Mühe gehabt, dieses Verdikt an der nächsten Generalversammlung überzeugend den Aktionären zu erläutern.

5. Schlussbemerkung

Obschon in Deutschland kein Sonderstrafrecht für Organe juristischer Personen existiert, besteht dennoch die Möglichkeit der Einziehung resp. des Verfalls von deren Vermögen gestützt auf § 75 DStGB unter dem Titel «Sondervorschrift für Organe und Vertreter». Die obersten Organe einer Gesellschaft hatten sich in der Schweiz bislang bei tatbestandsmässigem Handeln im Sinne von Art. 152 CHStGB strafrechtlich zu verantworten. Dabei wird das vorsätzliche Verbreiten von unwahren Angaben über den Lauf des kaufmännischen Gewerbes sanktioniert, wenn ein Dritter dadurch zu schädigenden Vermögensverfügungen veranlasst wird. In Analogie dazu bestehen seit 1976 im Deutschen Recht restriktivere Einzelnormierungen in §§ 264a, 265b sowie 298 DStGB. Seit der Schweizerischen Gesetzesnovelle vom 21. März 2003 (AS 2003 3043) sind die Gesellschaftsverantwortlichen nun neu auch mit dem Unternehmensstrafrecht in Art. 100^{quater} und 100^{quinquies} CHStGB konfrontiert. De lege ferenda haben die Organe in Deutschland dieselbe Sanktionierung zu erwarten. Insbesondere die Organisationsstruktur der Unternehmung, für welche der Vorstand, Aufsichtsrat oder Verwaltungsrat unmittelbar verantwortlich zeichnet, hat den neuen gesetzlichen Anforderungen zu genügen. Auch die Strafandrohung von bis zu CHF 5 Mio. sollte das oberste Gremium einer Unternehmung veranlassen, besonderes Augenmerk auf die Deliktsprävention innerhalb der Gesellschaft zu legen. Mit der Crime Due Diligence wird der Unternehmensführung ein Instrumentarium in die Hand gelegt, mit welchem sie wirksam Econ-Crime-Delikte von innen wie auch von aussen aufdecken kann. Wie bei jeder Technologierevolution, die das Leben der Menschheit nachhaltig verändert, versucht das Verbrechen, die neuen Möglichkeiten für seine Zwecke zu missbrauchen. Nachdem die Taterkennung dadurch schwieriger geworden ist, erhält jedermann, vom einfachen Kleinanleger bis zum Unternehmensführer, in Form der Crime Due Diligence ein Instrument, welches die Tat(früh)erkennung ermöglicht.