

TEIL V

Strafrechtliche Streiflichter

New Ecocrime* und New Economy

VON

DANIEL D. FISCHER**

Inhalt

1. Einführung
2. Begriff
 - 2.1 Historische Entwicklung
 - 2.1.1 Sicherheitsstandard und Kartengeld
 - 2.1.2 Technologie und Telekommunikation
 - 2.1.3 Neue Finanzinstrumente
 - 2.1.4 Anonymität des Internets
 - 2.2 Angloamerikanischer Einfluss
 - 2.3 New
 - 2.4 Eco
 - 2.5 Crime
 - 2.6 New Economy
 - 2.7 Neue Formen
 - 2.7.1 Hacken bzw. Cracken
 - 2.7.2 IT-Verbrechen
 - 2.7.3 IPO Initial public offering
3. Einzelne Phänomene
 - 3.1 Verlust der Unschuld der Betrüger
 - 3.1.1 Gewohnheits- und Einmaltäter
 - 3.1.2 Recovery Room Operations
 - 3.2 Irreführung der Opfer – Falscher Stolz
 - 3.2.1 Verträge
 - 3.2.2 Neue Finanzinstrumente
 - 3.3 Rolle der Anwälte
 - 3.3.1 Anwälte als Werkzeug
 - 3.3.2 Anwälte als Opfer
 - 3.3.3 Anwälte als Täter
 - 3.4 Rolle der Banken
 - 3.4.1 Banken als Werkzeug
 - 3.4.2 Banken als Opfer
 - 3.4.3 Banken als Täter

* Seit Februar 2002 Begriff geändert in Econcrime

** Der Autor dankt den Herren P. Cosandey, Chr. Weber und M. Glinig für ihre Anregungen und Mithilfe sowie seinem Assistenten, Herrn RA, lic. iur. P. Honold, für die Mitarbeit.

- 3.4.4 Verantwortung und Auftrag der Banken
- 3.5 Abwehrstrategie der Täter (counter attack)
 - 3.5.1 Angriff auf Opfer
- 3.6 Geschichte der Taten
- 3.7 Internet
 - 3.7.1 Mittel
 - 3.7.2 Abwehr
- 4. Einfluss auf die Wirtschaft (Overkill)
- 5. Beispielhafte Fälle
 - 5.1 Fall Boiler Room
 - 5.2 Fall Anlagebetrug
- 6. New Ecocrime und Recht
 - 6.1 Zuständigkeit der Schweizerischen Strafverfolgungsbehörden
 - 6.2 Rechtshilfe
 - 6.3 Betrug
 - 6.3.1 Arglist
 - 6.3.2 Gewerbsmässigkeit
 - 6.3.3 Betrug im Rahmen einer kriminellen Organisation
- 7. Massnahmen
 - 7.1 Intelligence
 - 7.2 Aufklärung
 - 7.2.1 Staat
 - 7.2.2 Banken
 - 7.2.3 Privat
- 8. Schlusswort

1. Einführung

Vielfach ist in der Entwicklungsgeschichte des Verbrechens davon die Rede, dass das Grundmuster der Straftat über die Jahrhunderte hinweg dasselbe geblieben ist. Dem Kriminellen stellen sich folgende drei Fragen:

- Wo hat es Geld?
- Wie komme ich leicht dazu?
- Wie entkomme ich?

In der Tat eben diese Fragen hat sich wohl schon Jesse James im 19. Jahrhundert beantwortet, genau so wie es die Zürcher Posträuber von 1997 getan haben. Insofern muss man denjenigen Recht geben, die meinen, es handle sich um neuen Wein in alten Schläuchen, wenn es darum geht, ob sich das Verbrechen im Laufe der Zeit verändert habe. Dies mag wohl zutreffen, wenn man sein Augenmerk auf die so genannten Brachialaneignungsdelikte, wie Raub oder Diebstahl, legt. Betrachtet man aber diejenigen Vermögensdelikte, wo der Straftäter seine Opfer durch eine List, m.a.W. *brain power*, schädigt (z.B.: Betrug, Veruntreuung), so zeigt sich freilich ein anderes Bild. Der Autor versucht nachfolgend aus der Sicht des Praktikers aufzuzeigen, dass sich das Verbrechen im Zuge von *New Economy* ebenfalls verändert hat und eine Art „new crime“, das *New Ecocrime*, entstanden ist.

2. Begriff

2.1 Historische Entwicklung

2.1.1 Sicherheitsstandard und Kartengeld

Um auf die drei eingangs erwähnten Fragen zurückzukommen: Die Antwort auf die erste fällt sicherlich einfach aus. Geld gibt es bei der Bank oder Post, wo sich das Risiko zum Überfall lohnt. Auf die immer raffinierteren Überfallstechniken reagierten die Geldinstitute mit immer höheren Sicherheitsstandards. Anfangs wurden die Schalter vergittert und/oder später mit Panzerglas geschützt. Man merkte aber schnell, dass beides der Kundennähe abträglich ist. Deshalb mussten andere Formen gefunden werden, dem Bankräuber möglichst zu erschweren, eine Antwort auf die zweite bzw. dritte Frage zu finden. Das Panzerglas verschwand wieder, dafür überwachten Videokameras den Schalteraum. Das Geld wurde vom Schalter weg in den gut geschützten Tresorraum verlagert. Mit Hilfe eines Röhrensystems konnte der Mitarbeiter am Bankschalter das Geld aus dem Tresorraum anfordern oder es dorthin zurückschicken. Bei ihm gab es ab sofort nichts mehr zu holen.

Der nächste grosse Schritt zur Verbesserung der Sicherheit war mit Bestimmtheit die Einführung des Kartengelds. Das Geld wurde entmaterialisiert. Die allermeisten monetären Transaktionen werden heute mit Buchgeld voll-

zogen. Es wäre ein Ding der Unmöglichkeit und ein Eldorado für jeden Bankräuber, wollte man bei den heutigen Summen, die jeden Tag rund um den Erdball verschoben werden, sämtliche Transaktionen durch das physische Überbringen von Geld abwickeln. Es wurden Geldersatzmittel eingeführt, die ohne die Unterschrift des Berechtigten oder eine Codennummer nichts wert sind. Natürlich bieten diese neuen Systeme vielfältige neue Möglichkeiten, sich fremde Vermögenswerte unrechtmässig anzueignen. Dafür braucht es aber mehr, als nur mit einer Waffe umgehen zu können.

2.1.2 Technologie und Telekommunikation

Fortschritte in der Technologie bringen immer eine Weiterentwicklung der Wirtschaft mit sich. Faxmaschinen, Mobiltelefone, Personalcomputer, Modem oder Internet sind heutzutage aus dem Berufsalltag nicht mehr wegzudenken. Aber auch Kriminelle wissen seit jeher diese Fortschritte für ihre Belange zu nutzen. Die Entwicklung der Wirtschaft geht Hand in Hand mit der Entwicklung des Verbrechens, Tempomacher ist dabei der technologische Fortschritt.

In den letzten Jahrzehnten erlebten wir einen wahren Technologiesprung. Vor allem auf dem Gebiet der Informationstechnologie und der Telekommunikation kann man von einer eigentlichen Revolution sprechen. Die Digitalisierung aller Informationen war der Startschuss zur Globalisierung der Wirtschaft. Die Möglichkeiten, welche die neuen Telekommunikationstechnologien bieten, machen das Wirtschaftsleben schneller, anonym und grenzenlos. Auf diesem Nährboden konnte eine neue Pflanze spriessen: die *New Economy* (siehe Punkt 2.6).

2.1.3 Neue Finanzinstrumente

Die Finanzinstrumente der Wirtschaft sind ebenfalls dem Wandel der Zeit unterworfen. Vor allem die vielen jungen Start-ups der *New Economy* bedürfen neuer Finanzinstrumente, die ihrerseits immer komplizierter aufgebaut sind. Hierbei die Übersicht zu wahren, fällt selbst Fachleuten schwer. Kleinanleger sind daher vielfach überfordert.

Waren es früher Aktien, Obligationen oder Warentermingeschäfte, unter denen der Investor wählen konnte, nahm ab den 70er Jahren des letzten Jahrhunderts die Vielfalt an Finanzinstrumenten stetig zu. Heutzutage hat es der interessierte Anleger mit einer Unmenge englischer Termini zu tun wie Structured Products, Derivatives, Options & Futures, Venture Capitals etc. Diese Liste könnte fast unendlich weitergeführt werden. Es erscheint klar, dass dieser undurchschaubare Wirrwarr an Begriffen eine ideale Basis für ausgeheckte Betrügereien bildet.

2.1.4 Anonymität des Internets

Das Internet bietet Zugang zu einer fast unbeschränkten Anzahl von Informationen. Diese Datenflut führt dazu, dass der einzelne Benutzer sich praktisch

anonym auf dem Netz bewegen kann. Über Internet ist es möglich, relativ billig und einfach an eine unbestimmte Zahl von potenziellen Opfern heranzukommen. Das Kosten-Nutzen-Verhältnis in Bezug auf Publicity ist unerreicht. Gerade das Internet ist ein Schulbeispiel dafür, dass sowohl die Wirtschaft wie auch das Verbrechen die Möglichkeiten, welche die Entwicklung neuer Technologien mit sich bringt, gleichermaßen für ihre Zwecke zu nutzen wissen. *New Economy* geht Hand in Hand mit *New Ecocrime*.

Logischerweise ist das Internet das ideale Tummelfeld des Verbrechens. Die dritte Frage, wie entkomme ich, stellt sich heute auf dem Internet kaum noch. Selbst wenn ein betrügerischer Betreiber einer Homepage auffliegt, ist es ihm ein Leichtes, bereits am anderen Tag eine neue Homepage unter einer neuen Adresse zu eröffnen und seine Machenschaften weiterzutreiben.

2.2 Angloamerikanischer Einfluss

Es ist in jüngster Vergangenheit so, dass neueste technische Errungenschaften, aber auch neue Entwicklungen in der Wirtschaft aus Amerika stammen. Meist erreichen solche Wellen von Neuentwicklungen via England Kontinentaleuropa.

Die Erfahrung in der Verbrechensbekämpfung zeigt, dass auch hier Parallelen zu erkennen sind. Kenner sprechen von einer Zeitverzögerung in der Größenordnung von ein bis zwei Jahren, in der dieselben Verbrecherphänomene in Europa auftauchen, mit welchen die amerikanischen Ermittler bereits zu tun hatten.

2.3 New

„As E-Commerce revolutionizes business, it also revolutionizes business fraud“ (KMPG Global e.fraud.survey 2001).

Die Digitalisierung der Informationen revolutionierte die menschliche Gesellschaft in all ihren Bereichen. Hand in Hand mit der technologischen Entwicklung entstehen für die Menschen neue Möglichkeiten fürs alltägliche Leben. Distanzen sind innert Sekundenbruchteilen überwindbar. Jedermann kommt leicht zur gewünschten Information über ein beliebiges Thema. Es ist klar, dass diese neuen, fast unbegrenzt erscheinenden Möglichkeiten auch unmittelbaren Einfluss auf die Entwicklung der Weltwirtschaft genommen haben (*New Economy*). Dieser Einfluss ist in jeder Sparte menschlichen Lebens zu spüren, so natürlich auch beim Verbrechen (*New Crime*).

2.4 Eco

Das Präfix „Eco“ steht für englisch „Economy“. Die Wirtschaft diktiert das Leben des Menschen seit der Industrialisierung im 19. Jahrhundert. Sie gibt das Tempo vor, an dem sich auch das Verbrechen orientiert. Das Hauptaugenmerk dieses Artikels soll auf dem Wirtschaftsverbrechen liegen.

2.5 Crime

In Anlehnung an den wirtschaftswissenschaftlichen Fachbegriff *New Economy* nennen wir diese neue Art von Wirtschaftsverbrechen *New Ecocrime*. Wie bereits unter Punkt 2.2 dargelegt, ist dieses Phänomen in den Vereinigten Staaten bereits seit längerem bekannt. Vielfach ist dort von Internet Fraud oder Cybercrime die Rede. U. E. ist dieser Begriff aber zu eng, da die neue Wirtschaftskriminalität sich nicht auf das Internet beschränken lässt, sondern im Zuge von *New Economy* entstanden ist.

2.6 New Economy

Der Begriff *New Economy* taucht bereits in der „Harvard Business Review“ aus dem Jahre 1993 auf und trat einen seither andauernden Siegeszug durch die weltweiten Medien an. In der Fachwelt schwelt seit geraumer Zeit ein Lehrstreit über die Frage, ob und inwiefern *New Economy* überhaupt existiert. Die Experten streiten sich vor allem über den Umstand, ob es dank den neuen technologischen Möglichkeiten zu einer Art Revolution in der Wirtschaft gekommen ist oder ob es sich vielmehr – auch hier – um neuen Wein in alten Schläuchen handelt. Die verschiedenen Lehrmeinungen manifestieren sich in der Fachpresse. Speziell die „Business Week“ redet der *New Economy* von allem Anfang an das Wort. Eher kritische Voten erscheinen im „The Economist“ und in der „Washington Post“. Dennoch scheint sich die Ansicht durchgesetzt zu haben, *New Economy* als wirtschaftswissenschaftliches Phänomen sei existent und als Fachterminus anerkannt, woran sich auch der Autor dieses Artikels orientiert. In seinem Aufsehen erregenden Grundsatzartikel „Auf der Suche nach der neuen Wirtschaft“ plädiert Gerhard Schwarz in der NZZ vom 18. März 2000 für eine differenziertere Optik auf die *New Economy*. Aus Sicht der Börse werden mit *New Economy* alle Unternehmen umfasst, welche Spitzentechnologie herstellen oder – wie E-Commerce – auf dieser beruhen. In ihrem makroökonomischen Sinn steht sie für die aussergewöhnliche Entwicklung der US-Wirtschaft und in ihrem Sog diejenige der Weltwirtschaft seit den 90er Jahren des letzten Jahrhunderts, in denen sich ein hohes Wirtschaftswachstum mit weitgehender Preisstabilität verband. Er wehrt sich dagegen, dass fundamentale Leitsätze der Wirtschaftswissenschaft ausser Kraft gesetzt worden seien. So gelten die Gesetze von Angebot und Nachfrage auch in der *New Economy* und hat jegliches Handeln in Zukunft seine Opportunitätskosten. Als neue Aspekte der jüngsten Entwicklung sind vielleicht das Tempo und Ausmass des wirtschaftlichen Wandels zu nennen. Letzten Endes ist die ganze Frage eine Problematik der Begriffsdefinition.

Laut „New Economy Index“ sind dreizehn Indikatoren für die neue Wirtschaft begriffsbildend:

1. *New Economy* ist gekennzeichnet durch flexible Produktion von Gütern und Dienstleistungen. Zum Vergleich: In der herkömmlichen Wirtschaftsordnung herrschte die standardisierte Massenproduktion vor.

2. Die Schere zwischen den hoch bezahlten Spezialjobs und den Billiglohnstellen für ungelernete Arbeitskräfte öffnet sich in der *New Economy* markant.
3. Die starke Zunahme des weltweiten Handels in der *New Economy* beschleunigt die Restrukturierung der Industrie- und Beschäftigungsstruktur.
4. Im Zeitalter der *New Economy* werden Investitionen weltweit getätigt. Die Allokation der Weltwirtschaftsgüter wird somit optimiert.
5. Ein Merkmal der *New Economy* sind die jungen, schnell wachsenden Unternehmen, die sog. Gazellen (Gesellschaften mit einer Umsatzsteigerung von mind. 20% im Vergleich zum Vorjahr innerhalb mindestens vier aufeinander folgender Jahre). Die Zeiten der Marktriesen mit einer jahrhundertelangen Firmentradition scheinen vorüber.
6. Der weltweite Wettbewerb hat markant zugenommen. Immer mehr Konkurrenten buhlen um die Marktanteile.
7. Unternehmungen der *New Economy* schliessen sich vermehrt zu Netzwerken, in Joint Ventures und/oder mittels Mergers zusammen, um Synergien zu gewinnen und gemeinsame Ziele anzustreben.
8. Die Firmengründungen und -schliessungen pro Jahr nehmen stetig zu.
9. Das Angebot in einem Marktsegment steigt in der *New Economy*. Der Konsument profitiert, indem seine Wünsche spezifischer abgedeckt werden.
10. Tempo ist das Mass aller Dinge der *New Economy*. Der Zeitzyklus für die Lancierung und Entwicklungen eines neuen Produktes wird kürzer.
11. New Economy basiert auf Microchips.
12. Der Einzug des Computers in die Geschäftswelt kreierte Unmengen von neuen Kosten und Jobs.
13. Die Kosten für den Datentransfer nehmen exponentiell ab.

2.7 Neue Formen

2.7.1 Hacken bzw. Cracken

Ursprünglich war der Begriff „Hacken“ nicht negativ besetzt. Er bedeutete vielmehr, die Fertigkeit des Programmierens auf hohem Niveau zu beherrschen. Der Hacker war sozusagen ein Experte in Sachen Computersprachen und -programmen. Bisweilen wurde der Terminus für so genannte Freaks gebraucht, welche die Programmstruktur von frei erhältlicher Software privat zu verbessern suchten. Mit dem Einzug des Internets Mitte der 80er Jahre wandelte sich der Sinngehalt. Hacken stand für das Eindringen in fremde Datenbanken unter Umgehung von Sicherheitsvorrichtungen. Der Hacker ist bestrebt, an sensible Daten zu gelangen, sei es aus wirtschaftlichem Interesse oder sei es auch nur als Herausforderung an die eigene Fertigkeit. Der korrekte Terminus für diese Tätigkeit ist aber „Cracken“. Er wurde in der breiten Öffentlichkeit mehr und mehr von „Hacken“ verdrängt, nachdem „Hacken“ in Tageszeitungen und Zeitschriften wiederholt fälschlicherweise verwendet wurde. Heutzutage ist es nicht mehr sinnvoll, am alten Begriff festzuhalten, da

sich Hacken im neueren Sinn so sehr eingebürgert hat, dass der ursprüngliche Terminus beinahe in Vergessenheit geraten ist.

Hacken ist in heutiger Zeit längst zu einem Industriezweig geworden. Vor allem nach dem Zusammenbruch der Sowjetunion verdingten sich Computerspezialisten für gutes Geld in den Westen. Unternehmen wie auch Staaten versprechen sich, durch das Hacken den technologischen Vorsprung der Konkurrenz auszugleichen. Der Schaden, der durch unerlaubtes Eindringen in Datenbanken weltweit entsteht, ist immens. Untersuchungen haben ergeben, dass etwa 50% der auf dem Internet präsenten Unternehmungen ihre Geschäftstätigkeit vor allen Dingen dadurch bedroht sehen, Opfer eines Hackerangriffs zu werden resp. die elektronischen Sicherheitsvorkehrungen zu wenig ausgebaut zu haben. Interessanterweise zeigt es sich, dass Opfer solcher Attacken in den meisten Fällen die rechtliche Verfolgung unterlassen. Dies vor allem aus zwei Gründen: Einerseits fehlen in den meisten Staaten die notwendigen Rechtsmittel und andererseits mangelt es den Geschädigten an Beweisen, um rechtlich vorgehen zu können. Der Täter bleibt so meist unerkannt (KMPG Global e.fraud.survey 2001).

2.7.2 IT-Verbrechen

Das IT-Zeitalter bietet den Marktteilnehmern viele neue Möglichkeiten, aber auch viele neue Möglichkeiten, sich gegenseitig rechtswidrig zu schädigen.

Hervorzuheben gelten hierbei vor allem die Computerviren. Sie sind eine neue Waffe im Köcher der Verbrecher. Es ist relativ leicht, damit einem Konkurrenten das Computersystem lahm zu legen. Der Aufwand zum Schutz gegen solche Attacken aus dem Netz wie auch für die Wiederherstellung eines befallenen Systems ist in finanzieller sowie in zeitlicher Hinsicht sehr gross.

Das amerikanische Justizministerium warnt besonders vor der Zunahme von betrügerischen Auktions- und Detailhandelswebsites auf dem Internet. Es wird hierbei hohe Qualität angepriesen und, nachdem der Kunde den Preis bezahlt hat, überhaupt nichts oder nur sehr schlechte Qualität geliefert.

Ebenfalls zu warnen ist vor so genannten „Work-at-home“-Angeboten. Per E-Mail oder auf Homepages werden Heimarbeitsjobs zu einer sehr hohen Entlohnung angeboten. Der interessierte Internetuser wird aufgefordert, einen hohen Geldbetrag als Depotleistung für das Arbeitsmaterial, das ihm zukommen soll, an den zukünftigen Arbeitgeber zu überweisen. Das Arbeitsmaterial wird nie geliefert.

Weiter zu nennen sind in der Rubrik Investment-Betrug der Verkauf von wertlosen Aktienpapieren aufgrund von manipulierten Aktienkursen („pump-and-dump“) oder in der Rubrik des Kreditkartenbetrugs die missbräuchliche Verwendung von Kreditkartennummern via Internet. Ebenfalls erwähnenswert ist die Industriespionage, welche in zunehmendem Masse durch das Eindringen in die Homepages durchgeführt werden kann.

In die Gruppe der IT-Verbrechen sind auch die unter Punkt 2.7.1 beschriebenen Hacker-Angriffe zu zählen.

2.7.3 IPO Initial public offering

IPO meint erstes öffentliches Angebot, d. h. Erstinanspruchnahme des inländischen Aktienmarktes auf dem Wege eines *going public*, einer Kapitalerhöhung oder einer Umlagerung. Es werden erstmalig Aktien eines Unternehmens interessierten Anlegern zum Kauf angeboten. Mit einem IPO ist im Allgemeinen eine Börsenzulassung des Aktienkapitals und die Kotierung an der Schweizer Börse verbunden. Aus Unternehmenssicht bedeutet ein IPO die Beschaffung von Risikokapital von aussen durch Nutzung der Aktie als Finanzierungsinstrument.

Zum Begriff „IPO“: Die Begriffsverwendung in der Rechts- als auch Wirtschafts-Literatur ist sehr uneinheitlich. Im englischen Sprachraum gelten die Termini *going public*, *Initial Equity Issues* oder *New Issues* als Synonyme. Ihnen entsprechen die deutschen Ausdrücke *Gang an die Börse*, *Börseneinführung*, *Öffnung*, *Neuemission* sowie *Erstemission*.

Es werden grundsätzlich zwei Arten von IPOs unterschieden: Einerseits kennt man das *Primary Offering*, wo neue Aktien für die Aktiengesellschaft geschaffen werden, und andererseits das *Secondary Offering*, wo ein Grossaktionär resp. Alleinaktionär seine Aktien ganz oder teilweise dem breiten Publikum zum Kauf anbietet. Der Hauptunterschied liegt darin, dass bei einem *Primary Offering* der vom Publikum bezahlte Preis der emittierenden Gesellschaft, bei einem *Secondary Offering* dagegen dem Verkäufer, d. h. dem Grossaktionär, zufließt (R. Watter, Die Festübernahme von Aktien, speziell beim „Initial Public Offering“). Hinzuweisen ist auf eine Unterart des IPO, das so genannte *Spin-off*. Dabei geht es um die Ausgliederung eines Unternehmens teils und Verkauf desselben an das Publikum (z.B.: Deutsche Telekom mit T-Online).

Ein Merkmal der *New Economy* ist die rasante Zunahme der IPOs. Es wurden neue Börsen wie NASDAQ, Nemax, SWX New Market etc. mit tieferen Zutrittskriterien geschaffen, um jungen Unternehmungen des neuen Markts die Möglichkeit zu bieten, ihre Aktien in einer breiten Öffentlichkeit zu streuen, um so eine möglichst hohe Kapitalisierungsquote pro Aktie anzustreben. Es liegt natürlich auf der Hand, dass die Lancierung von bislang unbekanntem Aktien mit hohen Gewinnaussichten für die Zukunft ein ideales Tummelfeld für allerlei Finanzbetrügereien bildet. Vor allem auf dem Internet werden IPO-Aktien von fiktiven E-Commerce-Gesellschaften als Geheimtipp gepriesen mit der Aussicht auf immense Kurssteigerung. Leider entpuppt sich derlei Geheimtipp oftmals als Luftschloss, der viele geprellte Kleinanleger auf wertlosen Aktien zurücklässt. Angesprochen sei hier die Boiler-Room-Problematik.

3. Einzelne Phänomene

3.1 Verlust der Unschuld der Betrüger

New Ecocrime zeichnet sich nicht nur dadurch aus, dass in den Methoden und im Umfeld deutliche Änderungen stattgefunden haben; begriffswesentlich ist vor allem, dass die Verhaltensmuster der Verbrechertypen markant von den bisher bekannten Verbrecherprofilen abweichen. Die Zeiten von Robin Hood, der quasi ein sozialistischer Umverteilungsverbrecher war, und die Wild-West-Romantik des Wells Fargo gehören der Vergangenheit an. Der Verbrecher mit einer hohen Sozialethik war schon früher die Ausnahme. Das Gegenteil aber, der dreiste *New-Ecocrime*-Täter, war ebenfalls kaum vorzufinden.

Zwei Grundprinzipien, an denen sich die Untersuchungsbehörden bis anhin orientieren konnten, waren: Lief gegen einen Kriminellen eine Untersuchung, gab er die kriminelle Aktivität auf, der Betrüger begab sich auf die Flucht bzw. stellte sein Machenschaften zumindest zeitweilig ein; hatte ein Krimineller ein Opfer bereits einmal erfolgreich betrogen und war bei diesem Opfer Schaden entstanden, liess er es danach in Ruhe.

Der skrupellose *New-Ecocrime*-Täter orientiert sich nicht an dem gegen ihn gerichteten Fahndungsdruck; trotz der polizeilichen Aktivitäten delinquent er weiter, schädigt Opfer gar ein zweites Mal. Die *New-Ecocrime*-Täter haben quasi ihre Unschuld verloren.

3.1.1 Gewohnheits- und Einmaltäter

Die Lehre unterschied bisher zwischen Gewohnheitsverbrechern und Situationstätern bzw. Wiederholungs- und Einmaltätern. Die Hintermänner des *New Ecocrime* passen nur bedingt in dieses Schema; sie sind kriminelle Berufs- und damit Gewohnheitsbetrüger. Begriffsrelevant ist aber die aussergewöhnliche Dreistigkeit während der Begehung der Straftat. Konkretisiert bedeutet dies, dass selbst eine Hausdurchsuchung in den Geschäftsräumlichkeiten des Betrügers oder die Verhaftung eines Mittäters ihn nur wenig beeinflusst. Seiner Delinquenz wird dadurch nicht Einhalt geboten. Früher wechselten diese Täter die Stadt, heute wechseln sie die Homepage oder den Server.

In den Rahmen dieser Dreistigkeit gehört auch die so genannte *counter attack*, auf welche in Ziffer 3.5 näher eingegangen wird.

3.1.2 Recovery Room Operations

Untersuchungen haben ergeben, dass das europäische Wirtschaftsverbrechen den amerikanischen Trends folgt und diese mit einer zeitlichen Verschiebung von wenigen Jahren kopiert, so auch die so genannten Recovery Room Operations. Darunter versteht man ein Begehungsmodell, in welchem der Täter von einem fixen Standort mittels Telefon oder Internet den Kontakt zum Opfer sucht. Entscheidend ist aber die diesbezügliche Zielrichtung. Bereits betrogene

Opfer werden erneut ins Visier genommen. Überraschenderweise ist diese Vorgehensweise erfolgreich, ist doch bekanntlich „das Letzte, das stirbt, die Hoffnung“.

Dem Geschädigten wird die Schadensrestitution in Aussicht gestellt. Bekannte Methoden sind einerseits die Form, in welcher ein neuer Täter mit Insiderwissen sich als der professionellere Berater vorstellt, oder der „reuige“ Erstbetrüger, der entschuldigend nun das wirklich sichere Geschäft präsentiert.

Im Gegensatz zu früher hält der Verbrecher nicht die Distanz zum geschädigten Opfer.

Das gute Geld wird entgegen dem Sprichwort dem Schlechten nachgeworfen. Diesen Verhaltensweisen der Opfer liegen einerseits das beschriebene spezifische Täterprofil und andererseits das spezifische Opferprofil zugrunde. Der Erfolg der Recovery Room Operations liegt nicht zuletzt darin begründet, dass dem überrumpelten Opfer Täter gegenüberstehen, welche eine hohe Eloquenz und Überzeugungsgabe auszeichnen. Diese Kriminellen haben keinerlei Hemmung und damit jegliche „Unschuld“ in ihrem Handeln verloren.

3.2 Irreführung der Opfer – Falscher Stolz

Eine sachgemässe, umfassende Prüfung wird oftmals dazu führen, dass die kriminelle Struktur eines Geschäftes erkannt wird. Indem *New-Ecocrime*-Täter sich untertänig gebären und dem Opfer gegenüber signalisieren, ihnen sei doch die Komplexität dieses Geschäftes bekannt, gelingt es ihnen häufig, die Opfer bzw. deren Berater dazu zu bringen, keine Abklärungen vorzunehmen. Gefördert wird dieser Verlauf durch die Aussicht auf den grossen Gewinn und die entsprechende Gier danach. Der Stolz des Opfers, seine Unkenntnis nicht zuzugeben, ist der Schlüssel für den Täter. Auch der zugezogene Berater vermeidet nicht zuletzt aus pekuniären Interessen die Manifestation seiner Unkenntnis. Diese psychologische Ausgangslage versetzt den Täter in eine bessere Position.

Erwähnung müssen auch die bekannten Konspirationsthesen finden; in diesem Rahmen ist vor allen Dingen auf den Handel mit Bankgarantien hinzuweisen (Prime Bank Instruments Fraud). Die Betrüger behaupten, die Banken würden selbst mit diesem (nicht existierenden) Handel hohe Gewinne erzielen, dies aber vor dem Kunden geheim halten. Zielgerichtet werden gewisse Vorbehalte gegen die Banken ausgenützt.

3.2.1 Verträge

Folge und Anwendungsbeispiel für das soeben beschriebene psychologische Phänomen ist die Unterzeichnung eines unverständlichen Vertrags. Dem Opfer bzw. dessen Anwalt werden häufig englischsprachige mehrseitige Vertragstexte vorgelegt, die einerseits kompliziert, mit Fachausdrücken versehen sind und andererseits einen professionellen Eindruck machen. Es bedarf mühseliger Abklärungen, um herauszufinden, dass diese Verträge keinen Sinn erge-

ben und sich widersprechen. Der zugezogene Berater sucht dann aber häufig den Fehler bei sich, weil er das Fachenglisch nicht so gut versteht. Dazu kommt, dass europäische Berater sich mit den umfangreichen amerikanischen Vertragstexten sehr häufig nicht auskennen.

Es fehlt nicht an Ironie, dass diese Vertragsbausteine unter den Betrügern gehandelt werden, was auf der anderen Seite für das Opfer den Vorteil hat, dass er betrügerische Texte an solchen Vertragsklauseln erkennen kann.

3.2.2 Neue Finanzinstrumente

Wie wir festgestellt haben, haben sich die gängigen Anlageformen ständig vermehrt und entwickelt. Kein Bankier bzw. Vermögensberater kann all diese neuen Produkte wirklich kennen. Es bedarf gelegentlich Mut, gegenüber seinem Kunden klar auszudrücken, dass der Gewinn mit unbekanntem Finanzinstrumenten eine Fiktion ist. Der Überbringer solcher schlechten Nachrichten ist häufig seine Beratungsfunktion los. Es ist wiederum der Stolz und die Eitelkeit und die Angst um die eigene pekuniäre Situation, die diesen Gutachter dazu verführen, nicht wirklich „gut“ zu achten.

Beispiele für diese fiktiven Bankgeschäfte sind unter anderem die nachfolgenden Termini:

- Bank Capability Letter
- Bank Debenture Program
- Bank Instrument Trading
- Blocked Assets Program
- Blocked Funds Letter
- Collateral First Medium Term Notes (MTN)
- FED-Pool Prime Bank Debenture Investments
- Medium Term Notes (MTN) Reserved Funds Letter

Es ist das Verdienst von Dr. Manfred Glinig, dass diese Termini zusammengetragen und publik gemacht worden sind. Darauf hingewiesen werden muss, dass es gelegentlich vorkommt, dass Gutgläubige in einem seriösen Geschäft solche Ausdrücke verwenden. Der Betrugsverdacht ist jedoch insbesondere dann dringend, wenn solche Begriffe in grosser Zahl im selben Vertragsdokument auftauchen.

3.3 Rolle der Anwälte

Bedauerlicherweise muss festgehalten werden, dass die Anwälte in den USA im Bereich des *New Ecocrime* eine Rolle spielen. Sie treten als Opfer, Täter, Mitäter sowie absichtliche und unabsichtliche Gehilfen auf. Gerade Europäer neigen dazu, eine Operation dann als seriös zu bewerten, wenn eine grosse Anwaltssozietät mit in das Geschäft involviert ist. Es gilt herauszustreichen, dass die Anwälte in den USA zweifelsfrei nicht jene hohe Reputation geniessen, wie das in Europa noch üblich ist. In den letzten zwei Jahren konnte festge-

stellt werden, dass die Gefährdung europäischer Anwaltskanzleien, von *New-Ecocrime*-Tätern missbraucht zu werden, stark gestiegen ist.

3.3.1 Anwälte als Werkzeug

Recht häufig nähern sich Kriminelle – unter Umständen durch private Kontakte – einem Anwalt an, geben ihm anfangs seriöse Aufträge und erschleichen sich so das Vertrauen. Ist dies einmal geschehen, ersuchen sie ihn beispielsweise, eine Gesellschaft zu gründen und in dieser als Verwaltungsrat zu wirken. Gleichzeitig werden gegen Entgelt die repräsentativen Räume des Anwalts als Firmendomizil der neuen Gesellschaft benutzt. Der Anwalt stellt in einem weiteren Schritt seine Bankbeziehungen zur Verfügung. Dadurch öffnet der Anwalt sein Kontensystem für möglicherweise diffuse Transaktionen und verstößt zusätzlich gegen das Geldwäschereigesetz. Anwälte müssen demnach beim Anbieten ausserprozessualer Dienstleistungen besonders vorsichtig sein. Damit wird von der lokalen Reputation und der Seriosität der Anwaltskanzleien profitiert und der Anwalt speziell bei Banken als „door-opener“ missbraucht.

Ähnlichen Gefahren sind auch Treuhänder, Notare, Vermögensberater und Personen mit einer hohen sozialen Reputation ausgesetzt. Es ist notwendig, dass sich diese Berufsleute ihrer neuen Gefährdung klar werden. In den Niederlanden werden insbesondere Anwälte und Notare in speziellen Seminaren auf diese Problematik geschult.

3.3.2 Anwälte als Opfer

Bei Bereitstellung oben genannter Dienstleistungen erwächst dem Anwalt, sofern er damit kriminelle Machenschaften begünstigt, eine erhebliche *reputation damage*. Seine Seriosität ist in der Zukunft in Frage gestellt. Im schlimmsten Fall kann es sogar zu einem Straf- und/oder Aufsichtskommissionsverfahren kommen.

Wenn hier aber vom Anwalt als Opfer gesprochen wird, soll noch ein weiteres Phänomen beschrieben werden: Die Geschädigten eines *New-Ecocrime*-Täters schliessen sich häufig zu einer Schadensgemeinschaft zusammen. Nur so ist es möglich, mit vernünftigem finanziellen Aufwand erfolgreich gegen die Täter vorzugehen.

Diese kennen die Opfer. Vielfach befinden sich die Täter in mehreren Staaten und die Kommunikation erfolgt über das Internet. Des Weiteren existieren auch Homepages, die als Informationsaustauschforum für Geschädigte dienen. Mehr und mehr versuchen nun die Betrüger, die anwaltliche Vertretung zu erschweren bzw. zu verunmöglichen. Die Kriminellen veranlassen, dass auf den genannten Homepages negative Informationen über die Opferanwälte verbreitet werden. Sie missbrauchen die Opferplattformen. Vor den Opferanwälten wird gewarnt und behauptet, sie würden effektiv zu den Betrügern gehören. Die potenziellen Klienten der Anwälte werden dahin gehend orientiert, dass sie diesen auf gar keinen Fall Vorschüsse zahlen sollen. Die Anwälte

würden sie nur übers Ohr hauen. Mit dieser Gegenstrategie erschweren die *New-Ecocrime*-Täter die Organisation der Opfergruppe erheblich.

Bekannt ist auch, dass die Betrüger selbst Anwälte einschalten, damit diese diejenigen Kollegen, welche die Opfer vertreten, anrufen, Einschüchterungsversuche unternehmen und insbesondere mit dem Gang an die lokalen Aufsichtsbehörden für Anwälte drohen. Es ist verständlich, dass manche Rechtsanwälte sehr wohl überdenken, ob sie Opfer vertreten oder weiterhin vertreten möchten.

3.3.3 Anwälte als Täter

Anwälte treten bedauerlicherweise gelegentlich als Drahtzieher oder Haupttäter von komplizierten schwer übersehbaren Betrugsangriffen auf die Anleger auf. Gerade in den letzten Monaten gab es zwei Aufsehen erregende Fälle (siehe Punkt 5.), in denen Rechtsanwälte aus dem angloamerikanischen Raum betrügerische Aktionen steuerten. Bei diesen Fällen darf aber nicht übersehen werden, dass die fraglichen Anwälte bereits vor Beginn ihres kriminellen Handelns ihre Fähigkeitsausweise verloren hatten, von ihrer beruflichen Tätigkeit her aber über ein wesentliches Know-how verfügten. Fokussiert muss die Tatsache werden, dass es sich *in casu* um Einzelfälle handelt, wobei der Schaden, der angerichtet wurde, enorme Ausmasse annahm. Statistisch gesehen ist aber keinesfalls Material vorhanden, das belegen würde, dass Advokaten häufig als Betrüger auftreten. Unter Ziffer 5 wird *in concreto* auf diese Sachverhalte einzugehen sein. Grundsätzlich empfiehlt es sich, jede Geldanlage, insbesondere wenn sie nicht von einem seriösen Geldinstitut angeboten wird, genauestens zu evaluieren. Hierzu gehören aber auch die Recherchen über den Offertensteller, unabhängig von der Rolle, die er einnimmt. *Due-Diligence*-Erhebungen sind nicht nur bei Betriebsübernahmen angezeigt, eine entsprechende Untersuchung gibt es auch im Finanzbereich, die von verschiedenen Fachanwälten angeboten wird. Es ist geradezu unsinnig, wenn jenes Geld, das mit seriöser, harter Arbeit, beispielsweise bei einer Betriebsübernahme, verdient wurde, dadurch verloren geht, dass man es auf unprofessionelle Weise, dem Prinzip der Hoffnung und Gier folgend, leichtfertig verspielt.

3.4 Rolle der Banken

Banken sind im engeren Sinn Anstalten oder Unternehmungen für Geldverkehr und Kreditvermittlung. Als Bankgeschäfte werden unter anderem genannt: Einlagen-, Kredit-, Diskont-, Effekten-, Depot-, Garantie- und Girogeschäft. Im Zusammenhang mit dem *New Ecocrime* zeigen sich die Banken, beziehungsweise Abteilungen von Banken, in den verschiedensten Facetten. Grundsätzlich geht es bei all diesen Betrügereien um Geld, wodurch die Geldinstitute in direkter oder indirekter Form betroffen sein können, nicht zuletzt dadurch, dass ihre Kontenstrukturen für kriminelle Vollzugshandlungen miss-

braucht werden. Eine Aufgabe, welcher die Banken offensichtlich nicht gewachsen sind, ist insbesondere die Beratung ihrer Kunden bei bankverwandten Anlagen. Nicht unerwähnt bleiben darf aber auch die Verantwortung der Banken für den Gesamtfinanzplatz. Banken sind leicht das Opfer betrügerischer Machenschaften gegen sie selbst, nicht zuletzt kommt es vor, dass kriminelle Aktionen durch Banken eingeleitet werden.

3.4.1 Banken als Werkzeug

New-Ecocrime-Täter suchen bewusst die Nähe von Bankinstituten. Es liegt ihnen viel daran, die Seriosität der Banken anzunehmen. Vor wenigen Monaten z.B. sollten mehrere Millionen DM gegen US-Dollar in Italien eingetauscht werden. Der Austausch würde in den Räumlichkeiten einer bekannten italienischen Bank durchgeführt werden. Man suggerierte damit den Eindruck, man mache das Geschäft mit der Bank. In Wahrheit fand die Austauschtransaktion in einem Teilbereich der öffentlich zugänglichen Schalterhalle statt. Die Bank war in dieses betrügerische Geschäft nicht involviert. Die Grösse der Empfangshalle dieser Bank liess aber nicht zu, dass der Vorfall den Bankverantwortlichen auffiel.

Die Banken sehen sich im Weiteren sehr häufig mit der Forderung konfrontiert zu bestätigen, dass das Geld bei ihnen auf einem Konto liegt und demnach in seriöser Form am internationalen Bankverkehr teilnimmt. Mehrfach kam es vor, dass die *New-Ecocrime*-Täter ihren Opfern mitteilten, sie könnten sich bei einer bestimmten Nummer bei der Bank über die Seriosität des Geschäftsvorschlags erkundigen. Selbstverständlich handelte es sich hier um eine gefälschte Visitenkarte und um einen Komplizen, der unter dem Namen der Bank unter dieser Nummer den Anruf entgegennahm und die Referenz stellte, ohne dass die Bank irgendetwas wusste.

In einem anderen Fall gingen Kriminelle erheblich raffinierter vor. Sie schleusten einen Gehilfen in die Zürcher Filiale einer renommierten ausländischen Grossbank ein, der dann wirklich namens der Bank Sachverhalte bestätigte, die dazu dienten, die betrügerische Position zu bestärken. Jener „echte-falsche“ Bankangestellte flog erst Jahre später auf. Wird auf Bankauskünfte verwiesen, empfiehlt es sich, solche Telefonnummern über öffentliche Verzeichnisse zu verifizieren bzw. sich über die Hauptnummer verbinden zu lassen.

Bankangestellte sehen sich auch gelegentlich mit der Forderung konfrontiert, aus Gefälligkeit von ihrem Fax aus einen Fax des Kunden abzusetzen. In der Regel sind solche Operationen unproblematisch. Es ist aber mehrfach vorgekommen, dass Betrüger unter Hinweis auf die echte Faxnummer der Bank ihre Glaubwürdigkeit zu verstärken versuchten.

Problematisch ist auch der Umstand, dass immer wieder versucht wird, Banken für das Halten von Treuhandkonti zu missbrauchen.

3.4.2 Banken als Opfer

Immer wieder wird versucht, Banken zu veranlassen, gefälschte Wertpapiere zu beleihen. Vor kurzem tauchten *Certificates of Deposit* der „Chase Manhattan Bank“ im Werte von 900 Mio. US-Dollar resp. zwei Billionen US-Dollar auf dem Bankenplatz Zürich auf. Andere Banken sollten dazu bewogen werden, diese Dokumente zu beleihen. Eine entsprechend durchgeführte *due diligence* ergab schwere formelle und materielle Mängel der besagten Zertifikate.

Mitte 2000 versuchte man, auf dem Bankenplatz Zürich ein Goldzertifikat betreffend kanadische Goldfunde über eine amerikanische und italienische Gruppe abzusetzen. Das *Certificate of Deposit* ging von Goldreserven von nicht weniger als 14 Billionen US-Dollar aus. Nebst den beträchtlichen formellen Mängeln kam die *Due-Diligence*-Abklärung zum Schluss, dass ein derartiger Goldfund eine absolute Weltsensation darstellen würde. Der grösste Goldfund, der in den letzten zehn Jahren weltweit gemacht wurde, hatte einen Wert von ca. 330 Mio. US-Dollar. Folglich war die Möglichkeit höchst unwahrscheinlich, dass ein Goldfund in der versprochenen Höhe tatsächlich existiert resp. dass die Weltöffentlichkeit von dieser Tatsache nichts wusste.

Daneben sehen sich die Banken regelmässig Schäden durch ungedeckte Checks, falsche Bankgarantien usw. gegenüber. Befragt man die zuständigen Security Departments der entsprechenden Banken über ihre Erfahrung mit *New-Ecocrime*-Delikten, antworten diese, der materielle Schaden, der den Banken, insbesondere den Grossbanken in der Schweiz, erwächst, sei gering, sofern sich die Mitarbeiter an die bankinternen Weisungen halten würden. Es wird die Frage zu beantworten sein, ob die Banken mit dieser Einstellung ihrer gesamtwirtschaftlichen Verantwortung genügend nachkommen.

3.4.3 Banken als Täter

So wenig wie sich Anwälte, Treuhänder und Vermögensberater im Bereich der *New Ecocrime* hervortun, genauso sehr gibt es aber immer wieder Banken, die in kriminelle Machenschaften auf diesem Gebiet verwickelt sind. Beispielsweise ist hierbei an die Manipulation von Aktienkursen zu denken. Ein solcher Fall trat vor kurzem bei der Zürcher Filiale einer grossen Auslandsbank auf; es war sogar ein führendes Geschäftsleitungsmitglied in die gesamte Affäre verwickelt.

Die Gefahr droht aber in erster Linie von anderswo. Genauso wie es möglich ist, mit wenig Kapital irgendwo irgendwie eine *Offshore*-Gesellschaft zu gründen, ist es möglich, teilweise mit weniger als 5'000 CHF Gründungskosten eine *Offshore*-Bank zum Entstehen zu bringen. Solche Institute werden mit Vorteil im südasiatischen Raum auf Klein- und Kleinstinseln, wie Tonga, Nauru, Western Samoa, Vanuatu, Montserrat und Cook-Islands, gegründet.

Die kriminelle Energie, die Gefahr, welche von den Hintermännern solcher Banken ausgeht, basiert vorwiegend auf dem Missbrauch, welcher mit den

Bankenfirmlen betrieben wird. In der Regel werden Opfer hellhörig, wenn derart exotische Bankinstitute auftreten. Tragen sie aber Firmen wie Rothschild Bank Ltd., Anguilla (Karibik), International Lloyds Bank oder Republic International Bank Ltd., glauben die Opfer häufig, es handle sich um die bekannten renommierten Bankinstitute. Die Anlehnung an die weltbekannten *brand names* geschieht natürlich in voller Absicht.

Die vorgenannten Ausführungen wollen auf keinen Fall besagen, dass alle Banken im süd pazifischen Raum kriminelle Hintermänner haben. Einzig soll darauf hingewiesen werden, dass bei solchen Finanzkonstrukten erhöhte Vorsicht geboten ist, evt. *Due-Diligence*-Abklärung nötig wird.

Ein anderes Kapitel ist die Gehilfenschaft von chinesischen bzw. Hong-Kong-chinesischen Bankinstituten, die darin besteht, dass *New-Ecocrime*-Täter ertrogene Summen dorthin überweisen lassen. Aufgrund der Tatsache, dass China keine staatsvertraglichen Pflichten akzeptiert, gehen die Opfer, selbst wenn die Täter identifiziert sind und das Betrugsdelikt offensichtlich ist, leer aus, da die chinesischen Banken zu keinerlei Hilfestellung bereit sind. Die Politik ist gefordert, durch entsprechende Massnahmen die „Gehilfenschaft“ Chinas zu unterbinden resp. den Abfluss krimineller Gelder dorthin zu verhindern.

3.4.4 Verantwortung und Auftrag der Banken

Nicht selten begeben sich die von den *New-Ecocrime*-Tätern angegangenen Opfer in einer ersten Reaktion zu ihrer Hausbank. Sie treffen dort auf einen Banker, der in der Regel mit der Komplexität internationaler Betrugsmodelle kaum vertraut ist. Es darf in diesem Zusammenhang auch festgehalten werden, dass die international operierenden Betrügerbanden untereinander Modelle austauschen und diese aufgrund der gemachten Erfahrungen updaten. Danach unternimmt der angefragte Banker eigene Kurzaufklärungen, deren Ergebnisse er seinem Kunden unter Hinweis darauf, dass in der Regel bankfremde Geschäfte so oder so nicht tauglich sind, vorträgt. Meistens macht der Bankier dem Kunden klar, das gesamte Machwerk sei unseriös, um dann mit dem Vorwurf zu enden, wie ein intelligenter Mensch einen solchen Unsinn überhaupt ernst nehmen kann. Sehr häufig führt dieses Gespräch dazu, dass sich der Kunde beleidigt fühlt, da man den nötigen Respekt ihm gegenüber missen liess und die Aufklärungen nur oberflächlich durchgeführt wurden. Da der Betrüger in der Regel ein Kommunikationstalent ist, ist es ihm ein Leichtes, dem Opfer klar zu machen, dass die Bank egoistisch vorging und dem Opfer nur ein gutes Geschäft missgönnte. Es kommt immer wieder vor, dass die Opfer dennoch das Geschäft abwickeln und auch ihre jahrelangen Bankbeziehungen auflösen. Dem wäre nicht so, hätte die Bank einen professionellen *Due-Diligence*-Bericht abgeliefert.

Wir haben festgestellt, dass *New Ecocrime* und Banken in fast allen Fällen in einer Verbindung stehen. Ein Faktum ist, dass *New-Ecocrime*-Kriminalität in der Schweiz ihren Anfang nimmt, da der Finanzplatz Schweiz im Ausland,

insbesondere was seine Seriosität und Geheimhaltung anbetrifft, eine hohes Ansehen genießt. Es wäre naiv zu glauben, dass die in der Schweiz stattfindende *New-Ecocrime*-Kriminalität unserem Finanzplatz nicht schadet. Es kann nicht angehen, dass die Banken sich damit begnügen festzustellen, sie betreffe die Angelegenheit nicht, da sie selbst nur einen kleinen Schaden davontragen. Gerade das Beispiel Liechtenstein zeigt, wie Verfehlungen Einzelner das Image des gesamten Finanzplatzes nachhaltig negativ beeinflussen können. Der Verband Österreichischer Banken und Bankiers ist beispielsweise dahin gehend aktiv geworden, dass er regelmässig Publikationen im Sinne einer präventiven Massnahme finanziell fördert. In England z.B. sind die Banken im Aufklärungsbereich erheblich aktiver.

Es stünde den Schweizer Banken gut an, wenn sie ihre gesamtwirtschaftliche Verantwortung für den Bankenplatz Schweiz ernster nähmen. Eine Beratungsstelle der Banken als Kontaktstelle für verunsicherte Kleinanleger wäre hierzu ein erster Schritt. Es genügt auf jeden Fall nicht, wenn beispielsweise wie im vergangenen Jahr eine einmalige Aufklärungskampagne unterstützt wird.

3.5 Abwehrstrategie der Täter (counter attack)

Analysiert man die Verbrecherbekämpfung in den letzten Jahren, treten die klassischen drei Parteien auf: zum einen die Untersuchungsbehörden, zum andern die Betrüger und schliesslich das Opfer. Sobald ein Strafverfahren läuft, gehen die Aktivitäten von den Strafbehörden aus, und zwar in Richtung Betrüger. Dieses Schema hat sich nun aber in den letzten Jahren verändert. Von Amerika aus inspiriert, greifen die *New-Ecocrime*-Täter die Strafbehörden bzw. die Anwälte sowie die Opfer an. Sie führen einen Gegenangriff, die sog. *counter attack*.

3.5.1 Angriff auf Opfer

mittels der Presse

Eine klassische Methode ist beispielsweise jene, bei der die Täter Pressekonferenzen abhalten und die Opfer damit publik machen und sie allenfalls in ein schlechtes Licht zerrren. Gute Beziehungen zu Journalisten können zu einem Schaden führen, welcher für das Opfer schwere Konsequenzen hat. Es kann durchaus vorkommen, dass sogar das Fernsehen eingeschaltet wird, Strafverfolgungsbehörden als voreingenommen und die Banken als die wahrhaft Bösen dargestellt werden. Häufig genügt die Drohung mit der Presse, um die Opfer einzuschüchtern.

wegen des Schwarzgeldes

Die gefährlichste Waffe der Betrüger ist aber die indirekte Drohung, dass eine Strafverfolgung dazu führen wird, dass der Ursprung der ertrogenen Gelder ans Licht kommt. Bekanntlich wird gerade steuerneutrales Geld bzw. Schwarzgeld bei ausserordentlichen Anlageformen verwendet. Nachdem es

dem Opfer in erster Linie um die Rückgewinnung des verlorenen Geldes geht und ein angestrebtes Strafverfahren dazu führen könnte, dass mögliche Steuerdelikte aufliegen, verzichtet das Opfer nicht selten auf die Strafverfolgung.

mit Prozessen

Dreist ist auch nachfolgende Methode: Sobald ein Opfer festhält, es sei allenfalls betrogen worden, wird ihm mit einem Prozess gedroht, da es mit dieser Aussage den guten Ruf des *New-Ecocrime*-Täters schädige. Dieser Drohung wird mit Schreiben von Anwälten Nachdruck verliehen. Meist werden sogar Prozesse in die Wege geleitet. Bis der Prozess wirklich entschieden ist, sind die Betrüger längst nicht mehr greifbar.

In Ziffer 3.3.2 wurde die *counter attack* gegenüber Anwälten und Opfern spezifisch behandelt. In 2.7.2 wurde auch auf die Gefahren der Computerviren hingewiesen, welche ebenfalls zum Arsenal der *counter attack* gehören.

3.6 Geschichte der Taten

Die Geschichte der Wirtschaftskriminalität ist von gut erkennbaren Modeströmungen begleitet. In den 70er Jahren des letzten Jahrhunderts waren es die Warentermingeschäfte, anfangs der 80er Jahre kamen die OTC (Over the Counter) Shares auf, aber auch das so genannte *venture capital* war damals in Mode. Nach dem Börsencrash von 1987 wurden Options & Futures als die neuen Finanzinstrumente gepriesen. In den 90er Jahren hatten die Strafuntersuchungsbehörden vor allem mit Aktienfälschung zu tun, wohingegen in heutiger Zeit gerade das Boiler Rooming (siehe unter Punkt 5.1) seine Blüte feiert.

3.7 Internet

Das Internet entstand 1959 durch Wissenschaftler und das Militär. Es verband, damals noch den Namen ARAP-NET tragend, Hunderte von Universitäten und staatlichen Einrichtungen. Im Jahre 1993 entwickelte das französische Institut CERN das World Wide Web und machte das Internet so auch Privatpersonen zugänglich. Das World Wide Web ist die multinationale Riesendatenbank des Internets. Mit Hilfe des WWW ist es möglich, die Informationen verschiedenster Anbieter in Form von Worten, Bildern, Sounds, Videos usw. darzustellen und Links zu anderen Seiten herzustellen. Das Internet ist so ein Riesennetzwerk, das mehr als hundert Millionen von Teilnehmern durch die Rechner miteinander verbindet. Fraglos wird dieses neue Informationsmedium noch bedeutender werden, als es heute schon ist. Als Kommunikationsmedium der Zukunft setzt es aber grundlegende Kenntnisse über Aufbau und Gefahren voraus. Der Begriff Internet leitet sich von Lateinisch „inter“, zwischen, ab. Das Internet ist also ein Zwischennetz, das bestehende, voneinander unabhängige Netzwerke zu einem globalen Netzwerk verbindet, so dass sie miteinander kommunizieren können. In unserem Zusammenhang

gesehen verbindet es auch *New-Ecocrime*-Täter mit anständigen Wirtschafts-subjekten.

Für Wirtschaftsunternehmen ist das Internet von entscheidender Bedeutung, denn unser auf Wettbewerb basierendes Wirtschaftssystem fordert immer schnellere Kommunikationsformen. Das Internet bietet hier eine im Vergleich zu anderen Technologien überlegene Plattform zum schnellen und günstigen Informationsaustausch. Es bedeutet einen Nachteil im heutigen Wettbewerb, das Internet nicht zur eigenen Präsentation, Kommunikation nutzen zu können.

Das Internet bietet sich aber auch als neues Kommunikationsforum für Straftäter an und damit einhergehend zur Plattform für die Begehung von Straftaten. *New-Ecocrime*-Täter versuchen hier dem Verfolgungsdruck, der in der realen Welt besteht, durch eine Flucht in das neue, anonymere Medium Internet zu entgehen und gleichzeitig die grösseren Verfügbarkeitsmöglichkeiten auszunutzen.

Spricht man von Internetkriminalität, denkt man in erster Linie an die Verbreitung und den Besitz von kinderpornographischen Dateien, an rechts- und linksextreme Inhalte, Software-Piraterie (illegale Bereitstellung von Musik, Computerprogrammen und bald auch digitalisierten Filmen im Internet) sowie Computersabotage.

Tauglichstes Mittel insbesondere gegen die Verbreitung problematischer Inhalte sind die so genannten Filtertechniken sowie das Rating. Damit werden problematische Angebote mit illegalem und jugendgefährdendem Inhalt verhindert. Die Europäische Union hat einen „Aktionsplan Internet“ lanciert, um gegen die Verbreitung dieser Angebote anzukämpfen. Wenn im Sinne von *New Ecocrime* von Internet die Rede ist, geht es in erster Linie um Hacking sowie die Wirtschaftskriminalität im Internet (siehe Punkt 2.7). Wir haben eingangs festgestellt, dass das Internet die weltgrösste Datenbank ist. Die grenzüberschreitende betrügerische Betätigung bietet den *New-Ecocrime*-Tätern neue und schädigende Möglichkeiten im Handel insbesondere mit Finanzdienstleistungen. Die Virtualität und Vielfalt des E-Commerce eröffnet einen Freiraum von Wirtschaftsdelikten unterschiedlichster Art. Das Internet ist aufgrund seiner Eigenschaft als Informationsforum für die kriminelle Nutzung bestens geeignet. Es ist eine Erfahrungstatsache, dass Kriminelle die Möglichkeiten rascher und intensiver nutzen als die Strafverfolgungsbehörden.

Die Verbreitung von gefälschten oder verfälschten Meldungen, die Eigen-darstellung krimineller Gesellschaften insbesondere dadurch, dass sie mit honorigen Firmen auf der Homepage verlinkt werden, bieten phantasievollen Tätern ein neues Instrumentarium, welches letztlich dazu führt, dass sich durch die Manipulation des Wirtschaftsmarktes *New-Ecocrime*-Täter auf unglaubliche Weise bereichern können.

3.7.1 Mittel

Wie ausgeführt, dient das Internet einerseits als Darstellungsmittel falscher Daten. Als Kommunikationsmedium hilft es dem raschen Informationsaustausch unter Wahrung strikter Anonymität. Bei der telefonischen Kommunikation kann man sich allenfalls von der Stimme her einen Eindruck verschaffen. Das Internet erlaubt von allem Anfang an eine gefärbte „Selbstpräsentation“. Ist man im Besitz eines ISDN-Telefonanschlusses, kann die Herkunft eines Anrufes lokalisiert werden. Beim Internet ist dies erheblich schwieriger. Nicht vergessen werden darf andererseits, dass die Betrügerei per Internet ausserordentlich preisgünstig ist und damit erlaubt, dass der Kreis der Betrugsadressaten quasi exponentiell zunimmt. Letzteres sei an einem bekannten Beispiel erläutert: Eine der bekanntesten *New-Ecocrime*-Betrugsformen ist der so genannte „Nigeria-Betrug“. Unaufgefordert erhält jemand per Fax oder per Post ein Schreiben, worin der Verfasser – zumindest ein hoher Beamter mit Dokortitel oder allenfalls sogar ein Prinz mit guten Verbindungen zur nigerianischen Zentralbank – den Empfänger ersucht, sein Geschäftskonto zur Abwicklung eines Geldtransfers zur Verfügung zu stellen, um dann einen beträchtlichen Gewinn zu erzielen. Geht das Opfer auf das Geschäft ein, hat es vorab eine Provision einzuzahlen. Selbstverständlich findet der Geldtransfer nie statt und das Opfer hat den Provisionsbetrag verloren. Auf diese plumpe Spielart des „Nigeria-Betrugs“ fällt heute kaum mehr jemand rein. In den letzten Jahren wurde er aber erheblich raffinierter gestaltet und verkompliziert.

Sofern der Betrugsversuch mittels Fax ergeht und angesichts der Tatsache der kleinen Treffermenge, entstehen dem Betrüger erhebliche Telefongebühren für Auslandsgespräche bzw. Faxe. Ist die Begehungsform der versandte Brief, sind die Portokosten erheblich. Wird aber, wie in letzter Zeit üblich, der „Nigeria-Betrug“ vorwiegend per E-Mail begangen, so sind die Kosten bedeutend tiefer. Als Konklusion kann festgehalten werden, dass die bisherigen Betrugsmodelle für die *New-Ecocrime*-Täter kostenattraktiver werden und neue Modelle dank des Internets entstanden sind.

3.7.2 Abwehr

Genauso wie das Internet Vorteile für die *New-Ecocrime*-Täter bietet, können aber auch Opfer bzw. Strafverfolgungsbehörden die Riesendatenbanken benutzen. Im World Wide Web findet man verschiedenste Foren und Listen der Geschädigten. Hier kann ein Informationsaustausch in dem Sinn, dass die Namen Krimineller hinsichtlich der Daten der Opfer ausgetauscht werden, stattfinden. Im Internet findet man zudem Listen von *New-Ecocrime*-Tätern.

Im Weiteren kann das Internet auch durch die einzelnen Strafverfolgungsbehörden benützt werden. Auf diese Weise kann Rechtshilfe auf dem informativen Weg erheblich an Schlagkraft gewinnen.

Im letzten Jahr ist eine Diskussion darüber entstanden, ob das Internet den *New-Ecocrime*-Tätern mehr nützt oder ob das Internet als Verfolgungsinstru-

ment ihnen mehr Schaden zufügt. Diese Frage ist vor allen Dingen eine akademische. Sie zu beantworten, ist nicht dringend notwendig. Wichtig ist nur, dass die Abwehrmöglichkeiten rigoros genutzt werden.

4. Einfluss auf die Wirtschaft (Overkill)

Es ist zweifelsfrei, dass *New-Ecocrime*-Delikte unsere Wirtschaft beeinflussen. Hunderte von Opfern werden geschädigt. Insbesondere muss das Wirtschaftssubjekt von einer bestimmten Wahrscheinlichkeit der Schädigung ausgehen und der Einzelne oder die Firma muss ein Sicherheitsdispositiv aufbauen, welches häufig in einem Missverhältnis zum Wirtschaftstransfer steht. Generell führt dies dazu, dass die Wirtschaft horrenden Ausgaben hat, um sich vor den Betrügern zu schützen.

Es gibt bis anhin keinerlei gesicherten Zahlen über den wirtschaftlichen Schaden, den *New-Ecocrime*-Täter anrichten. Nachdem beispielsweise Fälle bekannt sind (unter Punkt 5), wo es zu einem Schaden von bis zu 2 Milliarden US-Dollar kam, hohe Deliktbeträge also geradezu Kennzeichen des *New Ecocrime* sind, ist fraglos, dass die Schätzungen über Schadenssummen von mehreren Milliarden pro Jahr durchaus realistisch sind. Wesentlich ist aber insbesondere auch der immaterielle Schaden. Kommt ein Anwalt bzw. das Opfer in Verbindung mit einem solchen Verbrechen, kann es sein, dass das Wirtschaftssubjekt ein Leben lang stigmatisiert ist und man ihn als Geschäftspartner meidet, da es ins Umfeld der *New-Ecocrime*-Täter gehört.

Die Grundsatzfrage, die sich stellt, ist die, wie man richtig auf die Bedrohung durch *New Ecocrime* reagiert. Insbesondere besteht die Gefahr, dass die Massnahmen, die man trifft, letztlich im Ergebnis übertrieben sind, dass von Sicherheitsstandards viele betroffen sind, die absolut redlich Geschäfte tätigen. Beispielsweise wird gesagt, dass es empfehlenswert sei, bei Angehörigen von osteuropäischen Staaten erhöhte Vorsicht walten zu lassen. Dies kann aber dazu führen, dass ein Geschäft zum Beispiel mit einem Russen nicht zustande kommt, obwohl es legal ist. *Offshore*-Gesellschaften müssen durchaus nicht per se Struktur für kriminelle Handlungen sein.

Klassisches Beispiel dafür, dass Massnahmen manchmal zu weit greifen und die Wirtschaft behindern, ist auch das Schweizerische Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor, kurz Geldwäschereigesetz. Die Gesetzesbestimmungen sind im Ergebnis zu streng für den Normalbürger und zu large für die Kriminellen. Die Gesetzesdichte kann im Weiteren auch dazu führen, dass die *New-Ecocrime*-Delinquenten beim Opfer mehr Erfolg haben, da sie – beispielsweise gerade im Bereich des steuerneutralen Geldes – Opfer finden, die bereit sind, illegale Geldströme zu benützen. Inwiefern die US-Gesetzgebung betreffend die bankliche Registrierung jeder Summe über US\$ 10'000 notwendig ist, kann offen gelassen werden.

Fraglich ist auch, ob es sinnvoll ist, wie dies teilweise bei Bankinstituten in England gehandhabt wird, dass ein neuer Bankkunde ein Bankkonto nur er-

öffnen kann, wenn er zwei Referenzen angibt. Solcherlei Massnahmen können Jungunternehmer treffen, deren Fortkommen dadurch effektiv erschwert ist.

5. Beispielhafte Fälle

Zur Veranschaulichung des *New Ecocrime* sollen zwei Fälle dienen, die sich in jüngster Zeit zugetragen haben.

5.1 Fall Boiler Room

Ein internationaler Ring von Aktienbetrügern arbeitet über Websites im Internet. Es werden darauf Aktien angepriesen, insbesondere IPO-Aktien mit Aussicht auf hohe Rendite. Die Betrüger haben ein Netz von Briefkastenfirmen – verteilt über die ganze Welt – aufgezogen. Das „Mutterhaus“ liegt offenbar in den USA, aber operativ tätig werden sie über Firmen, die im südostasiatischen Raum angesiedelt sind. Es sind dies Firmen in den Wirtschaftszentren von Thailand und den Philippinen; in letzter Zeit treten aber auch immer wieder Adressen in Westeuropa (Spanien, Irland, Schweiz) auf. Ihr Marktauftritt ist auf ein betont seriöses Erscheinungsbild angelegt. Die interessierten Kleinanleger werden auf der Homepage mit hohen Gewinnversprechen gelockt. Es wird gesagt, dass die Aktien von prosperierenden Start-ups der IT-Branche herkommen, die den Gang an die Börse suchen, um neues Wachstumskapital zu generieren. In Tat und Wahrheit sind die besagten Firmen inexistent, resp. sie existieren nur als Briefkasten. Nachdem der Kleinanleger investiert hat, tritt das bekannte *Boiler-Room*-Phänomen auf. Die Aktienkurse werden künstlich gepuscht, vielfach steigen sie auch dank der grossen Nachfrage der geprellten Investoren. Mit sog. *feel-good-letters* werden die Opfer in Sicherheit gewiegelt und zu weiteren Investitionen gedrängt. Der Höhepunkt ist jeweils schnell erreicht. Sobald sich der Aktienkurs auf den Sinkflug begibt, versuchen die Kleinanleger verständlicherweise ihre Aktien zu verkaufen. Sie werden aber daran gehindert, indem die Aktienbroker nicht mehr kontaktierbar sind. Die Telefone sind tot, die Homepages abgeschaltet und E-Mails werden nicht beantwortet. Auf Nachforschung hin zeigt es sich, dass es die Firma an dieser Adresse nicht mehr gibt. Die Investoren bleiben auf den sich entwertenden Aktien sitzen und tragen so einen Riesenverlust. Die Aktienbroker sind aber längst wieder auf dem Netz unter einer neuen Homepage, Firma und Adresse tätig. Es kam schon vor, dass ein Kleinanleger über zwei verschiedene Gesellschaften derselben Betrügerbande um sein Geld gebracht wurde.

In einer zweiten Phase werden die frustrierten Opfer erneut (natürlich unter neuem Firmennamen) kontaktiert. Es wird ihnen ein Angebot unterbreitet, wonach sie ihre nunmehr wertlosen Aktien gegen andere Aktien – ebenfalls meist ein Geheimtipp des E-Commerce – für eine einmalige, aber happige Gebühr eintauschen könnten. So genannte Aktienbroker nehmen per Telefon

Kontakt auf und versuchen das Opfer zu überzeugen, das Angebot anzunehmen. Vielfach wird eine kurz bemessene Frist gesetzt, innert derer man sich zu entscheiden hat. Es werden hier ganz klar psychologische Mittel eingesetzt. Die Opfer haben bereits einen hohen Verlust verbuchen müssen, vielfach sind die ganzen Ersparnisse verloren. In einer solchen Situation versucht man sich an jeden rettenden Ast zu klammern, auch wenn dieser aus der Sicht des neutralen Beobachters zumindest als sehr morsch bezeichnet werden müsste. Das Geschäft der zweiten Phase nennt sich Recovery Room Operations.

5.2 Fall Anlagebetrug

Ein amerikanischer und ein kanadischer Anwalt führten in Zürich an bester Adresse eine grosse luxuriöse Anwaltskanzlei. Wie sich im Nachhinein herausstellte, war diese Kanzlei nur Fassade. Um den Eindruck auf die Kundschaft noch zu unterstreichen, stellten sie einen ganzen Stab von Sekretärinnen ein, die von den Machenschaften ihrer Vorgesetzten keine Ahnung hatten. Die Täter gaben sich als international tätige und äusserst erfolgreiche Investmentfachleute aus. Sie und ihre zahlreichen Helfer setzten englische Vertragswerke auf, die kein Mensch verstand, die aber Wunderbares versprachen: Gewinne in astronomischer Höhe, versicherte Risiken, Bankgarantien etc. So versuchten die beiden seriös und kompetent wirkenden Rechtsanwälte – teilweise mit erschreckendem Erfolg – den Anlegern sich selbst liquidierende Darlehen aufzuschwatzen. Diese neue Art von Geldvermehrung sollte angeblich so funktionieren, dass Kunden eine Geldleistung – als Gebühr oder Anzahlung – für ein Darlehen investieren, das derart gewinnbringend angelegt wird, dass weder Darlehenszinsen noch Unkosten bezahlt werden müssen; ja sogar die Rückzahlung des Darlehens selbst sollte hinfällig werden und für den Darlehensnehmer erst noch Gewinn abspringen.

Die Anwälte verwendeten für ihre Zwecke gefälschte Dokumente und Beglaubigungen, pflegten Beziehungen zu Banken, Versicherungen und Unternehmen auf der ganzen Welt und kauften in der Schweiz Aktienmäntel auf. Doch kein Rappen der gutgläubigen Anleger ist wie versprochen investiert worden. Das Geld ist einzig in die Taschen der Betrüger geflossen oder wurde zur Finanzierung der teuren Anwaltskanzlei direkt „re-investiert“. Bei den beiden Haupttätern handelt es sich um führende Mitglieder einer eigentlichen Finanz-Mafia, die mit grosser krimineller Energie und viel Phantasie vorgehen. Ihnen gelang es, bis zur Aufdeckung ihrer Machenschaften 7,6 Millionen Franken ahnungslosen Opfern abzunehmen. Insgesamt wurden allein in der Schweiz 38 Personen geschädigt.

Anhand dieses Beispiels zeigt sich die internationale Verflechtung des Verbrechens und die hohe Dreistigkeit des *New-Ecocrime*-Täters.

6. New Ecocrime und Recht

6.1 Zuständigkeit der schweizerischen Strafverfolgungsbehörden

Unter internationalem Strafrecht versteht man die Gesamtheit der Kollisionsnormen, welche den Anwendungsbereich des schweizerischen Strafrechts und die Zuständigkeit der schweizerischen Gerichtsbarkeit für Taten mit Auslandsbezug regeln (Franz Riklin, Schweizerisches Strafrecht, Zürich 1997, §8 N 15). Dieses Rechtsgebiet steckt noch in seinen Kinderschuhen. Das Völkerrecht hat kaum verbindliche Regeln zur Abgrenzung der Strafrechtshoheit zwischen den Staaten entwickelt. Die primäre Grundlage des internationalen Strafrechts ist das Territorialitätsprinzip: Der Staat ist für diejenigen Verbrechen zuständig, welche auf seinem Territorium verübt werden. Massgebend ist dabei der Ort, wo das Delikt begangen worden ist (Art. 3 StGB). Das mag zwar einleuchtend klingen, bedarf aber der Erläuterung für so genannte grenzüberschreitende Delikte, wie zum Beispiel jener Fall, wo ein Briefbombenbastler in der Schweiz das *corpus delicti* an seine Opfer ins Ausland schickt. Welcher Staat ist nun zuständig? Der Staat, in welchem die Ausführung der Tat begangen wurde, oder derjenige, in welchem der Erfolg der Tat eingetreten ist? Für solche Fälle gilt die Faustregel: Als Deliktsort gilt der Begehungsort, bei Erfolgsdelikten auch der Erfolgsort (Art. 7 StGB).

Die einzelnen Staaten bestimmen in autonomer Weise die Grenzen ihrer eigenen strafrechtlichen Zuständigkeit. Die momentane Diskussion um die Einsetzung eines internationalen Strafgerichtshofes und der erhebliche Widerstand, vor allem aus den USA, der diesem Vorhaben entgegenschlägt, zeigen, dass selbst in Zeiten der Globalisierung die Nationalstaaten ihre Bürger nur sehr zögernd einem fremden Strafgericht unterstellen wollen. Offenbar handelt es sich beim Strafrecht um ein besonders sensibles Rechtsgebiet, was der internationalen Koordination der Strafverfolgung eher abträglich ist. Gerade diese Tatsache ist stossend, denn im Zuge der globalisierten Wirtschaft, in der Wirtschaftsräume mit grenzenlosem Waren- und Personenverkehr entstehen, täte eine verbesserte internationale Koordination in der Strafverfolgung Not. Die Anstrengungen, zu welchen sich die Europäische Union mit der Unterzeichnung des Schengen-Abkommens verpflichtet hat (einheitliche Verbrecherdatenbank, schnellere Verfahren, gemeinsame Verfolgungsbehörden), sind ein positiv zu wertender Anfang. Auch in der Schweiz scheinen die Zeichen der Zeit erkannt, indem man versucht diesem Abkommen beizutreten.

6.2 Rechtshilfe

Für die Strafverfolgungsbehörden hört grundsätzlich die Arbeit an der Grenze auf. Danach beginnt ein langwieriger Marathon von Amt zu Amt und Gericht zu Gericht zur Erlangung von Rechtshilfe. Die Kriminellen wissen diesen Umstand sehr wohl für sich zu nutzen, wie das Beispiel von Ronald Biggs, dem

legendären britischen Posträuber, zeigt. Ihm gelang es, sich nach Brasilien abzusetzen. Der englische Staat hatte keine Möglichkeit mehr auf ihn zuzugreifen, da damals kein bilaterales Auslieferungsabkommen existierte. Heutzutage bestehen zwar mit praktisch allen Ländern Abkommen über die Rechtshilfe, dennoch beklagen die Strafverfolgungsbehörden die mangelnde Koordination. Infolge der grenzenlosen Mobilität der Verbrecher in den Wirtschaftsräumen hinken sie, die noch immer an die Staatsgrenzen gebunden sind, einen Schritt hinterher. Durch die Rechtshilfeverfahren verzögert sich die internationale Strafverfolgung und gerät in vielen Fällen zur Farce. Es ist bei weitem nicht so, dass lediglich die Zusammenarbeit mit den so genannten Bananenrepubliken im Argen liegt. Vielmehr ist auch die Kooperationsbereitschaft der Nachbarn in Westeuropa zu bemängeln. Hervorzuheben im negativen Sinn sind die Türkei, England, Italien und Spanien. Es sind dies alles Staaten, in welchen die nationale Souveränität besonders hohen Stellenwert genießt.

6.3 Betrug

Die Erfahrung zeigt, dass es sich bei *New-Ecocrime*-Delikten meistens um einen Betrugsstraftatbestand handelt. Es lohnt sich daher nachfolgend, Artikel 146 StGB auf seine *New-Ecocrime*-Tauglichkeit genauer zu untersuchen. Einen Betrug begeht, wer in der Absicht, sich oder einen anderen unrechtmässig zu bereichern, jemanden durch Vorspiegelung oder Unterdrückung von Tatsachen arglistig irreführt oder ihn in einem Irrtum arglistig bestärkt und so den Irrenden zu einem Verhalten bestimmt, wodurch dieser sich selbst oder einen anderen am Vermögen schädigt. Mit anderen Worten, ein Betrüger ist jemand, der in Bereicherungsabsicht einen anderen arglistig zu einer schädigenden Vermögensverfügung veranlasst.

Zur Erfüllung des Tatbestandes bedarf es somit folgender Tatbestandselemente: arglistige Täuschung, Irrtum, Vermögensdisposition, Vermögensschaden, Motivationszusammenhang zwischen Täuschung und Irrtum einerseits und zwischen Irrtum und Vermögensdisposition andererseits sowie Kausalzusammenhang zwischen Vermögensdisposition und Vermögensschaden.

6.3.1 Arglist

Der schweizerische Gesetzgeber folgte beim Erlass von Art. 146 StGB dem französischen Vorbild (Art. 313-1 Code pénal) und knüpfte an die Erfüllung des Betrugstatbestands ein zusätzliches Kriterium, nämlich die Arglist auf Seiten des Täters. Damit setzten sich die welschen Kantone gegenüber den deutschschweizerischen Kantonen durch, die in ihren Gesetzen den Betrugsstatbestand nach deutschem Vorbild kannten, wonach die einfache Lüge zum Betrug ausreicht. Der Hintergedanke zum Arglistkriterium entsprang dem Liberalismus. Es soll nur derjenige strafrechtlich geschützt werden, der sich mit einem Mindestmass an Aufmerksamkeit nicht selbst hätte schützen können

und den Irrtum durch ein Minimum zumutbarer Vorsicht hätte vermeiden können (BGE 99 IV 78; BGE 100 IV 274; BGE 119 IV 35). Eine einfache Lüge ist nach gängiger höchstrichterlicher Praxis nur dann arglistig, wenn

- sie nicht ohne besondere Mühe überprüfbar ist,
- dem Getäuschten die Überprüfung nicht zumutbar ist,
- der Täter den Getäuschten von der Überprüfung abhält oder
- der Täter aufgrund besonderer Umstände damit rechnet, dass das Opfer von einer Überprüfung absehen werde, ansonsten braucht es betrügerische Machenschaften.

Es braucht also betrügerische Machenschaften, die speziell perfid sind. Im höchstrichterlichen Sprachgebrauch nennt sich das Lügengebäude. Es zeigt sich in der Praxis, dass gerade das Arglistkriterium als hohe Hürde für die Beweisführung gilt. Vielfach scheidet eine Anklage an der beinahe vollständigen Unmöglichkeit, die Arglistigkeit nachzuweisen. Die Hürde wird verständlicherweise bei Delikten des *New Ecocrime* noch höher.

Arglist und Internet

Das Internet hat für Geschäftsbeziehungen von Anbeginn an einen etwas zwielichtigen Charakter gehabt. Die Tatsache, dass man seinen Geschäftspartner weder sehen noch hören kann, mahnt viele fast instinktiv zur Vorsicht, denn die Gegenpartei könnte theoretisch fast alles glaubhaft machen, ohne dass es nachgeprüft werden kann. Die Abneigung der Kunden, sich einem Unbekannten im Netz anzuvertrauen, machte vielen Verkaufsgesellschaften des sog. E-Commerce zu schaffen und dämpfte die Anfangseuphorie in dieser Sparte drastisch. Solange keine Sicherheit garantiert werden kann, schrecken viele (zu Recht) davor zurück, ihre persönlichen Daten bekannt zu geben, wie zum Beispiel die Kreditkartennummer, Name oder Adresse.

Vor diesem Hintergrund ist es für den Strafverfolger umso schwieriger, einem vermeintlichen *New-Ecocrime*-Betrüger die Arglist nachzuweisen. Der Verteidiger stellt sich dabei auf den Standpunkt, das Opfer hätte im Internet vorsichtiger agieren müssen, es war zu leichtfertig; von einem Lügengebäude zu sprechen, komme nicht in Frage, da das Opfer ein Mindestmass an Aufmerksamkeit missen liess. Handkehrum ist es für das Opfer gerade im Internet sehr schwer, den Geschäftspartner zu überprüfen und Geschäftsinformationen von unabhängiger Stelle zu bekommen. Doch als Gegenargument erscheint hier oft, dass gerade unter solchen Rahmenbedingungen eine erhöhte Sorgfalt am Platz ist. *New-Ecocrime*-Täter kommen so vielfach um eine Verurteilung wegen Betrugs herum.

Betrug ohne Arglist

Für den schweizerischen Gesetzgeber drängt sich damit die Frage auf, ob ein neuer, privilegierter Betrugstatbestand eingeführt werden soll, bei dem auf das Erfordernis der Arglist verzichtet wird. Der *New Ecocrime* verlangt nach neuen Wegen der Verbrechensbekämpfung. Die immer raffinierter agierenden

Täter vermögen die Opfer einzuwickeln und mit ihrer Überredungskunst zu Finanztransaktionen zu verleiten. Letztlich ist der Grat zwischen einer seriösen Finanzberatung und einer auf Betrugsabsicht basierenden ein sehr schmaler. Bei jeder Kapitalanlage schwingt ein gewisses Geschäftsrisiko mit. Vielfach ist es so, dass je höher die Rendite, desto höher auch das Risiko ist. Investiert zum Beispiel ein Kleinanleger auf Anraten eines Betrügers in einen IPO-Titel und sackt, nachdem die Luftblase im Boiler Room geplatzt ist, der Aktienwert in den Keller, so ist es für den Richter ein schweres Unterfangen zu entscheiden, inwiefern dieser finanzielle Schaden im unternehmerischen Risiko des Opfers liegt (Minimum an zumutbarer Vorsicht) und inwiefern der Schaden die Folge eines Betrages war. Genau an diesem Punkt liegt die Hürde des Arglistkriteriums sehr hoch. Der Autor plädiert deshalb in Anlehnung an das Deutsche Strafgesetzbuch § 263 für die Einführung eines privilegierten Betrugstatbestands, dem das Element der Arglist fehlt. Es würde dazu führen, dass mehr *New-Ecocrime*-Straftäter zur Rechenschaft gezogen würden. Eine übermässige Ausdehnung des Betrugstatbestandes ist insofern nicht zu befürchten, da letztlich in Deutschland dieselbe Praxis schon seit Jahrzehnten angewendet wird und entsprechend mehr Verurteilungen erfolgen.

6.3.2 Gewerbsmässigkeit

New-Ecocrime-Täter fallen vielfach unter die Sonderbestimmung von Art. 146 Abs. 2 StGB, wonach das Strafmass bei gewerbsmässigem Betrug verschärft wird. Nach der Umschreibung des Bundesgerichts ist die deliktische Tätigkeit gewerbsmässig, wenn der Täter die deliktische Tätigkeit nach der Art eines Berufes ausübt, so dass man angesichts der gesamten Umstände davon ausgehen muss, dass er „sich darauf eingerichtet hat, durch deliktische Handlungen Einkünfte zu erzielen, die einen namhaften Betrag an die Kosten zur Finanzierung seiner Lebensgestaltung darstellen“ (statt vieler BGE 119 IV 132 f.). Letztlich scheitert auch hier die Verurteilung wegen eines Betrugs an der Beweislosigkeit der Arglist. Zumindest für *New Ecocrime* bleibt dieser Artikel toter Buchstabe.

6.3.3 Betrug im Rahmen einer kriminellen Organisation

Des Öfteren wird beobachtet, dass *New-Ecocrime*-Täter organisiert vorgehen. Meist ist eine straffe Organisation erkennbar, die eine weltweite Tätigkeit abdeckt. In Art. 260ter StGB wird die Mitgliedschaft in einer kriminellen Organisation sanktioniert. Demnach ist strafbar, wer sich an einer Organisation beteiligt, die ihren Aufbau und ihre personelle Zusammensetzung geheim hält und die den Zweck verfolgt, Gewaltverbrechen zu begehen oder sich mit verbrecherischen Mitteln zu bereichern. Was unter einer kriminellen Organisation zu verstehen ist, bleibt im Gesetzestext offen. Die Materialien klären diesen Punkt insofern, als in der Botschaft (S. 281) folgende Definition abgegeben wurde: „Organisiertes Verbrechen liegt dort vor, wo Organisationen in Annäherung an

die Funktionsweise internationaler Unternehmen hochgradig arbeitsteilig, stark abgeschottet, planmässig und auf Dauer angelegt sind und durch Begehung von Delikten sowie durch die Teilnahme an der legalen Wirtschaft möglichst hohe Gewinne anstreben. Die Organisation bedient sich dabei der Mittel der Gewalt, Einschüchterung und Einflussnahme auf Politik und Wirtschaft. Sie weist regelmässig einen stark hierarchischen Aufbau auf und verfügt über wirksame Durchsetzungsmechanismen für interne Gruppennormen.“ Diese Umschreibung passt auf *New-Ecocrime*-Strukturen. Leider sind auch hier die Hürden hoch, um eine solche Organisationsstruktur jemals nachweisen zu können. Die Strafverfolgungsbehörden sind gefordert, das Merkmal der Organisation dem Angeschuldigten zu beweisen. Dafür ist es notwendig, dass sich mindestens drei Personen zusammenschliessen, um auf Dauer arbeitsteilig und planmässig tätig zu werden. Sollte dieser Nachweis gelingen, müssen in einem zweiten Schritt die verbrecherischen Mittel, welcher sich die kriminelle Organisation bedient, bewiesen werden.

Conspiracy nach amerikanischem Vorbild

Das amerikanische Recht kennt das qualifizierende Merkmal der *Conspiracy*. Im Federal Conspiracy Law werden komplotähnliche Gebilde schärfer bestraft. Es ist so, dass im amerikanischen Recht der mühsame Weg über den Extratratbestand der kriminellen Organisation erspart bleibt. Ähnlich wie im schweizerischen Strafrecht die Qualifizierung der Gewerbmässigkeit gehandhabt wird, wird das Vorgehen in einer *Conspiracy* vom amerikanischen Recht härter sanktioniert als der Grundtatbestand des in Frage stehenden Deliktes. Dies hat beispielsweise zur Folge, dass *New-Ecocrime*-Täter, die des Betruges überführt sind, eine Strafverschärfung zu gewärtigen haben, falls sie in einer kriminellen Organisationsstruktur aufgetreten sind.

7. Massnahmen

Der Autor fordert spezifische Massnahmen, um der *New-Ecocrime*-Problematik besser Herr zu werden.

7.1 Intelligence

Was im anglo-amerikanischen Raum bereits angewendet wird, sollte auch für Westeuropa gefordert werden, nämlich die Einrichtung von Intelligence Centres gegen die *New Ecocrime*. Wenn schon diese neue Art von Delikten aus den USA importiert wird, so sollten auch die Abwehrmassnahmen übernommen werden. Vom Erfahrungsvorsprung der amerikanischen Kollegen kann in Westeuropa nur profitiert werden. Im Jahre 1999 beispielsweise hat das amerikanische Justizdepartment eine so genannte „Internet Fraud Initiative“ gestartet. Sie soll bezwecken, dass das Justizdepartment rigoros verschiedene Fälle

von *New Ecocrime* verfolgt, aufdeckt und eine Verurteilung der Verantwortlichen anstrebt. Des Weiteren sollen die Anstrengungen national koordiniert und es soll auf bundesstaatlicher Ebene unter der Leitung des Justizdepartements kooperiert werden. Auch dieser Ansatz ist für die Schweiz zu fordern.

7.2 Aufklärung

7.2.1 Staat

In der Schweiz wurde letztes Jahr eine Informationskampagne in Zusammenarbeit mit der Bankiervereinigung gestartet, welche die breite Öffentlichkeit auf die Risiken der neuen Wirtschaftsdelikte aufmerksam machen soll. Die Zeichen der Zeit scheinen erkannt. Dennoch wird eine einmalige Aktion binnen Kürze in ihrer Wirkung verpuffen. Gefordert sind vielmehr permanente Massnahmen. Eine öffentliche Beratungsstelle bei der Wirtschaftspolizei brächte hier sicherlich Abhilfe. Wichtig ist, dass verunsicherte Kleinanleger anonymen Zugang zur Beratung haben.

7.2.2 Banken

Leider nehmen die Banken ihre Verantwortung, die sie einerseits für den Wirtschaftsstandort Schweiz und andererseits aufgrund ihrer Involvierung (siehe Punkt 3.4) in den *New Ecocrime* haben, zu wenig wahr. Der Schweizerischen Bankiervereinigung stände eine gewisse finanzielle wie auch personelle Aktivität in Sachen Prävention gut an. Zu denken ist hierbei an eine Anlaufstelle resp. einen Ombudsmann, die bzw. der ein Auge auf die *New-Ecocrime*-Szene hat und so vor neuen Modeströmungen rechtzeitig warnen kann. Verwiesen sei auch auf das gute Beispiel des Verbands Österreichischer Banken und Bankiers, der regelmässig Publikationen im Sinne einer präventiven Massnahme finanziell fördert. Seminare für Strafverfolgungsbehörden und Anwälte könnten die Sensibilität für *New Ecocrime* steigern. Banken sind sozusagen am Puls der Finanzwelt und verfügen somit über den besten Kenntnisstand.

7.2.3 Privat

In Presseerzeugnissen, mit denen man eine breite Öffentlichkeit erreichen kann, könnte im Wirtschaftsteil ein so genannter Warnbarometer eingeführt werden. Dieser – von einem Fachmann geführt – hätte die Funktion, auf neueste Modeströmungen des *New Ecocrime* aufmerksam zu machen. Viele potenzielle Opfer, vor allem Kleinanleger ohne grosse Insider-Kenntnisse, könnten so vor Schaden bewahrt werden.

Einfache Tipps sollten Internetbenutzern als Faustregeln mitgegeben werden:

Es sei grösste Zurückhaltung angebracht, wenn es darum geht, persönliche Daten, wie die Kreditkartennummer, auf dem Internet weiterzugeben. Besondere Vorsicht ist geboten bei Geschäftsbeziehung mit Internetbenutzern, die

ihre wahre Identität verbergen. Einer Aufforderung, einen Vorschuss ohne entsprechende Sicherheiten für irgendwelche unüblichen Gegenleistungen zu tätigen, sollte man in aller Regel nicht nachkommen.

8. Schlusswort

Der technologische Fortschritt der letzten Jahrzehnte brachte eine rasante Zunahme an Kommunikationsmöglichkeiten und an Geschwindigkeit des Datentransfers. Die Wirtschaft wusste diese Umstände zu nutzen, und es entwickelte sich die *New Economy*. Wie bei jeder technischen Revolution, die das Leben der Menschheit nachhaltig verändert, versucht das Verbrechen die neuen Möglichkeiten für seine Zwecke zu missbrauchen. Das Beispiel Internet zeigt sehr schön, dass einerseits ein neuer Wirtschaftszweig – E-Commerce – hat entstehen können und andererseits auch die Kriminellen mehr Werkzeuge bekommen haben. Letztlich ständen den Strafverfolgungsbehörden diese Möglichkeiten ebenfalls offen, doch muss festgestellt werden, dass sie hier dem Verbrechen einen Schritt hinterherhinken. Zudem kämpfen sie mit einem zusätzlichen Hindernis, nämlich den Staatsgrenzen, welche für die *New-Ecocrime*-Delinquenten dank des grenzenlosen World Wide Web leicht zu überwinden sind.

New Economy ist existent, *New Ecocrime* zweifellos auch. *New Ecocrime* bedroht die *New Economy*. Soll verhindert werden, dass *New Ecocrime* geradezu ein Kennzeichen des neuen Wirtschaftssystems ist, ist es unumgänglich, die geforderten Massnahmen zu treffen.

