Geldwäsche – Money Laundering

Robert F. J. Harnischmacher
Consultant in Security
and Intelligence Matters
International Security
and Media Consulting
Associate Editor of
the World Police
Encyclopedia, New York

Scheinfirmen

Damit die Herkunft von Geld nicht mehr nachvollzogen werden kann, wird es mittels einer unübersichtlichen Vielzahl von Transaktionen verschickt. Dabei landet das Geld meist auf dem Konto einer ausländischen Scheinfirma, die nur zu diesem Zwecke dient, aber keine Produkte oder Leistungen erbringt. Die ausländische Scheinfirma bezahlt dann Rechnungen einer weiteren Scheinfirma in Deutschland. Die Rechnungen sind aber nur fingiert – sie enthalten nicht erbrachte Leistungen. Die deutsche Firma macht somit satte Gewinne, die sie wiederum legal versteuert. Diese legal versteuerten Gewinne der Scheinfirma können dann ohne Probleme in den Wirtschaftskreislauf eingeschleust werden.
Je nachdem, ob die bankenrechtliche oder die gesellschaftsrechtliche Sichtweise im Vordergrund steht, unterscheidet man zwischen “Bank Havens“ und “Company Havens“. Bank Havens sind Off – Shore – Plätze, in denen es sehr einfach ist, eine Bank oder ein Finanzinstitut zu eröffnen. Diese Off – Shore – Banken können, müssen aber nicht, den Einleger- oder Kreditbetrug erleichtern. Hingegen stellen Company Havens nur sehr geringe Anforderungen an die Gründung von Scheingesellschaften. Die Geldwäsche und ihr globaler Einfluss auf Wirtschaftsstrukturen
Nicht erst seit dem 11. September 2001 wissen wir um die Macht der Geldwäsche. Mit diesem Datum wurde ein Buch mit dem Arbeitstitel “La verite´ interdite“ (“Die verbotene Wahrheit“ – Die Verstrickungen der USA mit Osama bin Laden) von Jean – Charles Brisard und Guillaume Dasquie´ hochbrisant, dass das Abgleiten saudi – arabischer Finanznetze in den Terrorismus und die engen Bande, die im Kern dieser Netze zwischen den bin Ladens und den bin Mahfouz bestehen, aufzeigen, ebenso werden aber auch die Verbindungen zahlreicher Persönlichkeiten aus der Umgebung des ehemaligen US – Präsidenten George Bush und des vorherigen Präsidenten, seines Sohnes George W. Bush, beschrieben zur Spitze der Carlyle – Group – Investmentgesellschaft, zu der auch ein Vertrauter Bin Ladens zum Vorstand zählt. Finanziers, die zu den ehrbarsten der Welt zählen, eine Familie, die am Aufbau des saudi – arabischen Königreichs mitwirkte, afghanische Freundschaften, die eher auf Opportunismus als auf strategischen Überlegungen beruhen, verborgene Verbrechen in Libyen, die mit Freunden der britischen Krone begangen wurden, ein Mann, der vom FBI verfolgt, aber vom State Department verschont wird, der von den führenden westlichen Politikern angeprangert, aber von Oberst Gaddafi gejagt wird, Taliban – Freunde, mit denen sich die US – Diplomatie immer wieder versöhnt, bevor sie bombardiert werden – Osama Bin Laden hat von all dem etwas. Er kämpft mit den Waffen, die ihm der Westen anvertraut hat, er hat sich Subversion, Guerilla und Propaganda als modus operandi zu eigen gemacht, um die höchsten Werte in “seiner Welt des Denkens und Empfindens und Glaubens“ zu verteidigen, “gnadenlos, koste es, was es wolle“, weil die Öldiktaturen vollkommen überholte Glaubenslehren begünstigen, auch durch offene oder verdeckte Zahlungen als Paymaster Terroristen unterstützen. Insofern erscheint die Erdölpolitik der letzten 50 Jahre in der kritischen teleologischen Betrachtung mehr als ambivalent, auf die unsere wirtschaftliche Entwicklung im Westen beruht. Und so nutzt er natürlich auch in seinem Finanzgebaren das Off – Shore – Banking mit viel Zugewinn mit seinen weltweit verzweigten Verbindungssträngen und Netzstrukturen, zu denen auch mafiose Strukturen zählen, die wiederum mit ihrem Geld die Finanzwelt Osama Bin Ladens in Rotation halten, wo Geldwäsche der “Stein der Weisen“ ist.
“Das größte Hindernis bei den Ermittlungen gegen islamistische Terroristen waren die Interessen der US – Ölkonzerne und die Rolle Saudi – Arabiens“ (so John O’Neill, bis August 2001 beim FBI mit den Ermittlungen gegen bin Laden beauftragt. Er starb am 11.09.2001 im World Trade Center). Electronic – Banking – money laundering per Datentransfer Um die Maßnahmen der Geldwäschebekämpfung im Bereich der unbaren Transaktionen zu verbessern und die dort noch bestehenden Umsetzungsdefizite zu beseitigen, hat die sog. aktive Nachforschungspflicht (Research) sowie die Beobachtung (Monitoring) von unter Geldwäschegesichtspunkten auffälligen Geschäftsbeziehungen besondere Bedeutung. Hierbei handelt es sich um das sogenannte “Know – your - customer – Prinzip“ (auch “Conozca su cliente – Prinzip“ im Spanischen genannt). Jeder Cyber – Attacke kann ein Sturzflug folgen. Wenn es denen gelänge, datengestützte Finanz-, Wirtschafts-, Verkehrs-, Versorgungs- oder (militärische) Führungssysteme zu zerstören, vermögen sie ein Ausmaß an kosten- und ggf. todbringendem Chaos zu erzeugen, das mit Waffen- und

Sprengstoffeinsätzen schwer zu erzielen wäre. Jedes Raketenabwehrsystem wäre schon im Entwicklungsstadium wertlos. Hier gibt es keine Frontlinie.
Das Elektron wird die ultimative präzisions - gesteuerte Waffe der Zukunft sein. Die Waffen des “Information warfare“ sind meistens Computersoftware, beispielsweise so genannte “logische Bomben“ und “eaves-dropping sniffers“ oder hochentwickelte elektronische Hardware, z.B. die “High-Energy-Radio Frequency Device“, bekannt als HERF-Waffe. Sogar die CIA wurde schon im Internet angegriffen und zwölf Stunden lang haben Hacker das Dokumentationszentrum der CIA mit dem “Playboy“ verlinkt, sodass statt der Dokumentation immer wieder Bilder von nackten Frauen erschienen. 2001 gelang es einem 15 – jährigen Hacker aus Michigan, drei Mal in Rechner der Raumfahrtbehörde NASA einzudringen und Websites zu verändern. Einer Hackergruppe gelang es vor drei Jahren sogar, einen britischen Aufklärungssatelliten mehrere Stunden unter Kontrolle zu bringen ! Erste Anzeichen eines eigentlichen “Cyber – Terrorismus“ waren z.B. 1998 die Bombenanschläge der “Provisional IRA“ im Londoner Börsenviertel und den Docklands, die ganz gezielt Infrastrukturknoten zum Ziel hatten. Man schätzt für die letzten zwei Jahre die materiellen Schäden auf ca. 3,6 Milliarden US – Dollar, wobei die Dunkelziffer weit höher liegen dürfte.
In Deutschland sollen solche Attacken 1990 noch 160 Millionen DM Schaden betragen haben, für das Jahr 2000 wurden Kosten von ca. 500 Millionen DM für die Behebung von Viren – Schäden geschätzt. Die Zahl solcher Viren– und Hackerangriffe, die zunehmend politischer Art und Natur sind, nimmt weltweit zu: Waren es 1992 nur 773, wurden bis Oktober letzten Jahres 21.756 bekannt ! Feindliche Mächte und Terroristen können somit einen Laptop in eine grauenhafte Waffe mit riesigen und verheerenden Schadensfolgen verwandeln ! So schon US – Präsident Clinton Anfang 2000. Das Internet bietet für Terroristen und Geldwäscheprofis der O.K. geradezu ideale und perfekte “Arbeitsbedingungen“. Warfare ist längst Realität geworden. Das Internet löst die alten traditionellen Schlachtfelder ab und wird selbst zum Kampfplatz. “Wer mit zehn Panzerdivisionen keine Chance hat, hat sie womöglich mit zehn Hackern“. In einem anno 2001 von der chinesischen Luftwaffe in Guangzhon herausgegebenen Buch kann man eindrucksvoll nachlesen: “Information Warfare ist ein wichtiger Faktor geworden und entscheidet über den Ausgang eines Krieges“. “Hacker sind nicht mehr nur daran interessiert, Dienste zu behindern oder Viren einzupflanzen“, erklärt Frost & Sullivan Analystin Brooks Lieske, und ergänzt: “ Sie betreiben auch weniger auffällige, aber potenziell schädigendere Aktivitäten wie das Lesen von Bilanzen, Konten eMails und das Ausspionieren von Internetseiten und Computern“. Oberstes Gebot, so die Experten der Nachrichtendienste und einschlägigen Wissenschaften ist daher der Auftrag an die Sicherheitsfachkräfte, ein sensitiveres Gefahrengefühl zu entwickeln zur Vorbeugung und Verhinderung von imaginären und tatsächlichen Schadenseintritten durch Missbrauch unbefugter Dritter zum Nachteil der Institution oder Firma. Was durchweg fehlt, ist ein ausreichendes Risiko- und Sicherheitsbewusstsein. Die Opfer machen es dem Angreifer leicht, da viele Unternehmen und Behörden ihre Schutzmaßnahmen nicht regelmäßig auf den neuesten Stand bringen. Zumeist wächst der Leichtsinn der Nutzer auch mit dem zeitlichen Abstand zum letzten Computer - Gau. Nach US-Studien werden lediglich vier Prozent aller digitalen Einbrüche überhaupt bemerkt ! Würde der dominante Internet - Knotenpunkt in Frankfurt am Main, an dem die Leitungen aller deutschen Netzwerk - Betreiber zusammenlaufen, Ziel eines Anschlags, hätte das dramatische Konsequenzen für die hiesige Nutzung des Internets. Was wäre, wenn die Großbanken eines Landes auf Grund elektronischer Manipulationen in die Zahlungsunfähigkeit getrieben würden ? Oder gar, wenn ein Staat einen anderen massiv mit elektronischen Mitteln angreifen würde?
Makaberes klassisches Beispiel zur Datenausspähung beziehungsweise zur Manipulation in einem fremden Rechner anno 1993: Ein Computervirus hatte die Ergebnisse des Escobar-Untersuchungsausschusses im US-Senat – wenige Stunden, bevor sie der Öffentlichkeit präsentiert werden sollten, gelöscht. Das meldete der britische Informationsdienst “Virus News“. Kokain-König Pablo Escobar war am 22. Juli 1992 aus dem Gefängnis “La Catedral“ in Kolumbien geflohen. Es ist festzustellen, dass sich wie ein roter Faden seit 1990 das Eindringen von Hackern auch in Polizeicomputer, angefangen von der DEA in den USA über Scotland Yard bis hin zur kolumbianischen Gerichtspolizei vollzieht. Wieder der Beweis, dass die OK wahrlich alles an Möglichkeiten nutzt, was ihren Unternehmungen und Geschäften und natürlich deren Schutz und Absicherung effektiv nutzt. Der Wandel der Bank der Zukunft durch Online-Banking und Elektonic-Banking zu einer Netzwerk-Bank ist längst erkannt und schon
durch verschiedene Beispiele entwertet, wo es z.B. russischen Computerspezialisten gelang,

über das Telefonnetz in das elektronische Überweisungssystem der Citibank-Computer vierzigmal einzudringen und mehr als zehn Millionen Dollar auf Konten in Finnland, Russland, Deutschland, den Niederlanden, den USA, Israel und der Schweiz zu überweisen (so das FBI). Der Cyber-Angriff auf zentrale, zum Beispiel wirtschaftliche Computersysteme bei Banken, Börsen und anderen, kann man als "größte Gefahr für die Sicherheit" einschätzen, nicht weil es der ehemalige US - Präsident Bill Clinton so formuliert hat im Mai 1998 in einer Rede vor Absolventen der Marine-Akademie in Annapolis. Clinton erklärte, diese neuen Gefahren hätten inzwischen die atomare Bedrohung des Kalten Krieges abgelöst. Er forderte, schnell ein System gegen Computerangriffe zu entwickeln.
Bei der Analyse der weltweiten Zahlungsbilanzen ist aufgefallen, dass ihr Saldo nicht wie theoretisch angenommen null ist, sondern ein großes "schwarzes Loch" in ihrer Verrechnung besteht. Jährlich kommen Exporte im Wert von 50 Millionen US – Dollar nirgendwo in der Welt an. Sie werden in einem Land als Export registriert, ohne in einem anderen Land als Import gemeldet zu sein. Im Zeitraum von 1967 bis 1987 wurden 1.000 Milliarden US - Dollar bei internationalen Transaktionen überwiesen, ohne dass ein Land den Erhalt dieser Summe deklariert hat. Diese Summe entspräche ungefähr der Verschuldung der Dritten Welt. Ebenfalls wurden für Zinsen, Dividenden und Schiffsfracht jährlich einige Milliarden US – Dollar an unbekannte Empfänger überwiesen. Als Ursache für dieses schwarze Loch wird zu 2/3 die Anhäufung eines riesigen Vermögens aus illegalen Geschäften gesehen, das sich anscheinend in einem Niemandsland befindet und somit nirgendwo besteuert wird. Dieses Niemandsland spiegeln die Off – Shore – Zentren wider. Bei einer Kapitalausfuhr aus einem Industrieland wird diese nur teilweise, die Einfuhr in das Off – Shore – Zentrum überhaupt nicht registriert. Umgekehrt wird eine Kapitaleinfuhr nur in dem Industrieland, nicht aber in dem Off – Shore – Zentrum vermerkt. Den die Zahlungsbilanzen verzerrenden Einfluss von Geldwäsche auf gesamtwirtschaftliche Erhebungen genau abzuschätzen, ist fast unmöglich, jedoch ist zu vermuten, dass sie zu beträchtlichen Verfälschungen führen und damit die Aussagekraft statistischer Erhebungen mindern. Da diese Daten aber oft die Grundlage nationaler und internationaler politischer Entscheidungen bilden, können sie zu falschen ökonomischen Analysen und (wirtschafts-) politischen Fehlentscheidungen führen. So wird durch die Rückführung gewaschener Drogengelder von Off – Shore – Banken in die ursprünglichen Anbauländer eine Erhöhung ihres eh meist schon enormen Schuldenbergs bemerkt. Bildet sich, so wie in Bolivien, eine besonders starke Untergrundwirtschaft durch Drogenhandel aus, verringert sich die Aussagekraft offizieller Banken und Statistiken auf ein Minimum. Außerdem wird vermutet, dass speziell durch den Drogenhandel Ressourcen aus Dritte – Welt- und Schwellenländern zu relativ niedrigen Preisen abgezogen werden, sich aber die gewaschenen Gewinne aufgrund höherer Verzinsung und Sicherheit in den reicheren Industrieländern und Off – Shore – Zentren ansammeln. Damit wird das weltweite Ungleichgewicht weiter gestört.
Die mit gewaschenen Geldern erlangten riesigen Kapitalbestände können gewinnbringend , sicher und legal integriert, aber auch in Form von Spekulationskapital gezielt als ökonomisches und politisches Druckmittel eingesetzt werden. Durch die immensen Geldbeträge, die das organisierte Verbrechen kurzfristig bewegen kann, kann der Kapitalmarkt durch An- und Verkauf von Devisen, Aktien und festverzinslichen Wertpapieren stark manipuliert oder gar lahm gelegt werden.
Der Einsatz hoher Geldbeträge bei relativ niedrigem Kursniveau ermöglicht bedeutende Kursgewinne. Dagegen lässt ein umfangreicher Verkauf von Wertpapieren zur gleichen Zeit die Kurse sinken. Der Kauf von Staatsanleihen und – obligationen kann eine gefährliche Abhängigkeit des Staates vom organisierten Verbrechen entstehen lassen. Diese Abhängigkeit kann leicht dazu führen, dass Staatsregierungen erpressbar werden, wie dies ansatzweise in Italien und Bolivien bereits geschehen ist.
Die organisierte Kriminalität in ihrer angehäuften Form ist eine finanzielle Marktmacht, die zur Bedrohung des legalen Wettbewerbssystems führen kann. Durch das fast unbegrenzte Investitionsvolumen, welches auf die enormen Gewinne aus Geldwäscheaktivitäten zurückzuführen ist, könnte es soweit kommen, dass nicht derjenige den wirtschaftlichen Erfolg aufweist, der das bessere Produkt anbietet, sondern derjenige, der über die größeren, illegalen Finanzmittel verfügt. Die Investitionen werden nicht nach rationalen Gesichtspunkten getätigt, sondern es wird lediglich eine Optimierung der Infrastruktur der organisierten Kriminalität und Gewinn legalisierende Reinvestition angestrebt.
Das zentrale Problem ist der Missbrauch des Bankgeheimnisses für kriminelle Zwecke, der zum einen die Glaubwürdigkeit und Stabilität der Banken gefährdet und zum anderen den Staat zu Maßnahmen zwingt, die die Autonomie der Banken und das Bankgeheimnis schwächen. Das Bankwesen ist der Sektor der legalen Wirtschaft, der am meisten in die

Geldwäsche involviert ist und zugleich bedroht und beeinflusst wird. Die Banken befinden sich in einem Interessenkonflikt. Einerseits wollen sie den Ruf vermeiden, besonders hart gegen Geldwäsche vorzugehen, um keine potenziellen Kunden abzuschrecken; andererseits müssen sie den Eindruck vermeiden, eine Bank der organisierten Kriminalität zu sein, um nicht das Vertrauen ihrer Kunden und damit deren Einlagen zu verlieren. Zudem können Banken dem Wettbewerbsdruck und der Unterwanderung durch die organisierte Kriminalität zum Opfer fallen, indem sie von der organisierten Kriminalität missbraucht oder übernommen werden. Daher ist es zur Erhaltung der Stabilität des Finanzsystems unerlässlich, die Banken vor einer Gefahr zu schützen, an der sie auf den ersten Blick mitverdienen. Die für Finanzdienstleistungen erhaltenen Provisionen und Margen fallen bei den großen Geldmengen, die bei der Geldwäsche eingebracht werden, meist sehr groß aus, so dass die Banken erheblich daran verdienen können. Da die Erträge der Banken jedoch zugleich Kosten für die Geldwäscher darstellen, sind diese besonders daran interessiert, sich in Banken und Finanzbetriebe einzukaufen oder diese ganz zu übernehmen.

Ausklang

Anzumerken bleibt: Die Profite krimineller Vereinigungen werden weiter steigen. Nach Schätzungen westlicher Geheimdienste finanziert sich auch die Bundesregierung bei ihrer alljährlichen Kreditaufnahme schon jetzt zu 20 - 30 % aus dem Organisierten Verbrechen. Dies gilt auch für andere europäische Staaten, wird aber von den Regierungen gern verschwiegen oder heruntergespielt. Auch bei weniger kostenintensiven Dienstleistungen, wie etwa bei der Überweisung, ist es im Falle der Mitwisserschaft des Instituts üblich, bis zu 10 % an Provision zu vereinnahmen“. Man braucht auch diese horrenden Summen der kriminellen Hintermänner, denn je mehr Geld, aus welchen Quellen auch immer, auf den deutschen Markt drängt, um so niedriger bleiben die Zinsen“. Das rechtliche, organisatorische und technische Instrumentarium der USA besteht in keinem westeuropäischen Staat !! Dabei obliegt es der Politik und damit mittelbar dem Bürger zu entscheiden,

- ob die polizeilichen Informationssysteme stärker ausgebaut werden sollen,
- ob z.B. der “große Lauschangriff“ rechtlich ermöglicht wird,
- ob die Polizei- und sonstige Strafverfolgungsbeamten besser ausgebildet und bezahlt werden, um ein Abwandern von qualifizierten Beamten in die Industrie zu verhindern und Fachkräfte aus dem Wirtschaftsbereich (Buchhalter, Finanzexperten) zu gewinnen,
- ob Verdeckte Ermittler berechtigt sind, Straftaten zu begehen,
- ob Strafverfolgungsbehörden personell verstärkt werden,
- ob finanzielle Transaktionen bei Banken und Anwälten überprüft werden können,
- ob der Datenschutz teilweise zurückgeschraubt oder weiter ausgebaut wird,
- ob das Verfahren für die Sicherstellung von illegal erworbenen Vermögenswerten mit einer Beweislastumkehr versehen wird usw.

Dabei kann und sollte keine dieser Maßnahmen für sich gesondert betrachtet werden. Wer z.B. einen hohen Datenschutzstandard haben will, muss entsprechend Personal und Technik zur Verfügung stellen. Wer keinen “Lauschangriff“ will, muss in Kauf nehmen, dass gewisse Ermittlungsergebnisse und vor allem Beweismöglichkeiten gegen die Chefs bzw. die Hintermänner des organisierten Verbrechens nicht erbracht werden können. Wer keine Beweislastumkehr für die Sicherstellung von illegal erworbenen Vermögenswerten will, muss andere Ermittlungsmöglichkeiten wie z.B. personell und finanziell aufwendige Intelligence-Verfahren zur Verfügung stellen. Mit traditionellen Mitteln können wir das organisierte Verbrechen nicht mehr erfolgreich bekämpfen. Das haben unsere Nachbarstaaten inzwischen besser erkannt.

Fazit

Die internationale Geldwäsche hat sich trotz aller initiierten Gegenmaßnahmen zu einer Wachstumsbranche entwickelt. Aktuelle Ereignisse wie der zunehmende Anstieg der organisierten Kriminalität in der Welt, die Diskussionen um die Schwarzgeldkonten, die Aufspürung der Millionen aus der Oetker – Entführung, die Euroeinführung und die verschärften Maßnahmen nach dem 11. September 2001 in den USA zur Entdeckung von Geldwäscheaktivitäten zur Austrocknung der materiellen Basis der Terrorismusszene und organisierten Kriminalität gleichermaßen, spiegeln diese Tatsache deutlich wider. Fakt ist, die Geldwäsche ist ein fester Bestandteil der internationalen Wirtschaftsordnung und könnte nur wegen ihrer teuflischen Heirat mit der organisierten Kriminalität und mafiosen Netzwerken und terroristischen Überzeugungsstraftätern im Sinne eines

charismatischen Führers wie Osama bin Laden rigoros mit allen Mitteln bekämpft werden.